Produkthandbuch

McAfee ePolicy Orchestrator 5.3.0 – Software

COPYRIGHT
Copyright © 2014 McAfee, Inc. Keine Vervielfältigung ohne vorherige Zustimmung.

MARKEN
McAfee, das McAfee-Logo, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, Foundscore, Foundstone, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee Total Protection, TrustedSource, VirusScan, WaveSecure sind Marken oder eingetragene Marken von McAfee, Inc. oder der Tochterunternehmen in den USA und anderen Ländern. Alle anderen Namen und Marken sind Eigentum der jeweiligen Besitzer.

Produktnamen, Funktionsbezeichnungen und Beschreibungen können jederzeit unangekündigt geändert werden. Die jeweils aktuellen Informationen zu Produkten und Funktionen finden Sie unter mcafee.com.

INFORMATIONEN ZUR LIZENZ

Lizenzvereinbarung
HINWEIS FÜR ALLE BENUTZER: LESEN SIE DEN LIZENZVERTRAG FÜR DIE VON IHNEN ERWORBENE SOFTWARE SORGFÄLTIG DURCH. ER ENTHÄLT DIE ALLGEMEINEN BESTIMMUNGEN UND BEDINGUNGEN FÜR DIE VERWENDUNG DER LIZENZIERTEN SOFTWARE. WENN SIE NICHT WISSEN, WELCHEN SOFTWARE-LIZENZTYP SIE ERWORBEN HABEN, SCHLAGEN SIE IN DEN UNTERLAGEN ZUM KAUF UND WEITEREN UNTERLAGEN BEZÜGLICH DER LIZENZGEWÄHRUNG ODER DEN BESTELLUNTERLAGEN NACH, DIE SIE ZUSAMMEN MIT DEM SOFTWAREPAKET ODER SEPARAT (ALS BROSCHÜRE, DATEI AUF DER PRODUKT-CD ODER ALS DATEI, DIE AUF DER WEBSITE VERFÜGBAR IST, VON DER SIE AUCH DAS SOFTWAREPAKET HERUNTERGELADEN HABEN) ERHALTEN HABEN. WENN SIE MIT DEN IN DIESER VEREINBARUNG AUFGEFÜHRTEN BESTIMMUNGEN NICHT EINVERSTANDEN SIND, UNTERLASSEN SIE DIE INSTALLATION DER SOFTWARE. SOFERN MÖGLICH, GEBEN SIE DAS PRODUKT AN MCAFEE ODER IHREN HÄNDLER BEI VOLLER RÜCKERSTATTUNG DES KAUFPREISES ZURÜCK.

Inhaltsverzeichnis

Einleitung **11**
Informationen zu diesem Handbuch 11
Zielgruppe 11
Konventionen 11
Quellen für Produktinformationen 12

Einführung in McAfee ePolicy Orchestrator

1 Schützen Ihrer Netzwerke mithilfe von ePolicy Orchestrator **15**
Vorteile von ePolicy Orchestrator 15
Komponenten und ihre Funktion 15
Funktionsweise der Software 16

2 Verwenden der ePolicy Orchestrator-Benutzeroberfläche **19**
Anmelden und Abmelden 19
Navigieren in der Benutzeroberfläche 19
Verwenden des ePolicy Orchestrator-Navigationsmenüs 20
Anpassen der Navigationsleiste 20
Server-Einstellungskategorien 20
Arbeiten mit Listen und Tabellen 22
Filtern einer Liste 23
Suchen nach bestimmten Listeneinträgen 23
Aktivieren der Kontrollkästchen von Tabellenzeilen 24

Einrichten von ePolicy Orchestrator

3 Planen der ePolicy Orchestrator-Konfiguration **27**
Erwägungen zur Skalierbarkeit 27
Verwenden mehrerer McAfee ePO-Server 27
Verwenden mehrerer remoter Agentensteuerungen 28
Internetprotokolle in einer verwalteten Umgebung 28

4 Einrichten des McAfee ePO-Servers **31**
Überblick über die Server-Konfiguration 31
Verwenden des Status der automatischen Produktinstallation 33
Grundlegende Funktionen für die manuelle oder geführte Konfiguration 34
Konfigurieren grundlegender Funktionen 35
Verwenden eines Proxyservers 38
Eingeben Ihres Lizenzschlüssels 38
Konfigurieren von Product Improvement Program 38
Deinstallieren von McAfee Product Improvement Program 39

5 Benutzerkonten und Berechtigungssätze **41**
Benutzerkonten 41

Verwalten von Benutzerkonten . . . 41
Unterstützte Formate für Benutzernamen und Kennwörter . . . 42
Erstellen einer benutzerdefinierten Anmeldenachricht . . . 43
Konfigurieren einer Active Directory-Benutzeranmeldung . . . 43
Das Audit-Protokoll . . . 48
Client-Zertifikatauthentifizierung . . . 50
Verwenden der Client-Zertifikatauthentifizierung . . . 50
Konfigurieren von ePolicy Orchestrator für die Client-Zertifikatauthentifizierung . . . 51
Ändern der zertifikatbasierten Authentifizierung von McAfee ePO-Server . . . 51
Deaktivieren der Client-Zertifikatauthentifizierung von McAfee ePO-Server . . . 52
Konfigurieren von Benutzern für zertifikatbasierte Authentifizierung . . . 52
Aktualisieren der CRL-Datei . . . 53
Probleme bei der Client-Zertifikatauthentifizierung . . . 54
SSL-Zertifikate . . . 54
Erstellen eines selbstsignierten Zertifikats mit OpenSSL . . . 57
Weitere nützliche OpenSSL-Befehle . . . 59
Konvertieren einer vorhandenen PVK-Datei in eine PEM-Datei . . . 60
Berechtigungssätze . . . 61
Das Zusammenspiel von Benutzern, Gruppen und Berechtigungssätzen . . . 61
Verwalten von Berechtigungssätzen . . . 62

6 Repositories 65

Repository-Typen und ihre Funktion . . . 65
Typen verteilter Repositories . . . 67
Repository-Zweige und ihre Verwendung . . . 68
Repository-Listendateien . . . 69
Zusammenarbeit von Repositories . . . 70
Erstmaliges Einrichten von Repositories . . . 70
Verwalten von Quellsites und alternativen Sites . . . 71
Erstellen von Quellsites . . . 71
Wechseln zwischen Quellsites und alternativen Sites . . . 72
Bearbeiten von Quellsites und alternativen Sites . . . 72
Löschen von Quellsites oder Deaktivieren alternativer Sites . . . 73
Sicherstellen des Zugriffs auf die Quellsite . . . 73
Konfigurieren von Proxyeinstellungen . . . 73
Konfigurieren von Proxyeinstellungen für McAfee Agent . . . 74
Konfigurieren von Einstellungen für globale Aktualisierungen . . . 75
Konfigurieren von Agenten-Richtlinien zum Verwenden eines verteilten Repositorys . . . 76
Verwenden von SuperAgents als verteilte Repositories . . . 77
Erstellen von verteilten SuperAgent-Repositories . . . 77
Replizieren von Paketen in SuperAgent-Repositories . . . 78
Löschen von verteilten SuperAgent-Repositories . . . 78
Erstellen und Konfigurieren von Repositories auf FTP- oder HTTP-Servern und UNC-Freigaben . . . 79
Erstellen eines Ordnerspeicherorts . . . 80
Hinzufügen des verteilten Repositorys zu ePolicy Orchestrator . . . 80
Vermeiden der Replizierung von ausgewählten Paketen . . . 82
Deaktivieren der Replizierung von ausgewählten Paketen . . . 82
Aktivieren der Ordnerfreigabe für UNC- und HTTP-Repositories . . . 83
Bearbeiten von verteilten Repositories . . . 83
Löschen von verteilten Repositories . . . 83
Verwenden von UNC-Freigaben als verteilte Repositories . . . 84
Verwenden von lokalen verteilten Repositories, die nicht verwaltet werden . . . 85
Arbeiten mit den Repository-Listen-Dateien . . . 86
Exportieren der Repository-Listen-Datei SITELIST.XML . . . 87
Exportieren der Repository-Liste zur Sicherung oder für die Verwendung auf anderen Servern . . . 87

Importieren verteilter Repositories aus der Repository-Liste . . . 88
Importieren von Quellsites aus der Datei SITEMGR.XML . . . 88
Abruf-Tasks . . . 88
Replizierungs-Tasks . . . 89
Repository-Auswahl . . . 90

7 Registrierte Server 91
Registrieren von McAfee ePO-Servern . . . 91
Registrieren von LDAP-Servern . . . 93
Registrieren von SNMP-Servern . . . 94
Verwenden von Datenbank-Servern . . . 95
Registrieren eines Datenbank-Servers . . . 96
Ändern einer Datenbankregistrierung . . . 96
Entfernen einer registrierten Datenbank . . . 96
Freigeben von Objekten zwischen Servern . . . 97
Exportieren von Objekten und Daten aus dem McAfee ePO-Server . . . 97
Importieren von Elementen in ePolicy Orchestrator . . . 97

8 Agentensteuerungen 99
Funktionsweise von Agenten-Handlern . . . 99
Verbinden eines Agenten-Handlers in der DMZ mit einem McAfee ePO-Server in einer Domäne . . . 100
Steuerungsgruppen und -priorität . . . 101
Verwalten von Agentensteuerungen . . . 102
Zuweisen von McAfee Agents zu Agentensteuerungen . . . 102
Verwalten von Agentensteuerungszuweisungen . . . 103
Erstellen von Agentensteuerungsgruppen . . . 104
Verwalten von Agentensteuerungsgruppen . . . 104
Verschieben von Agenten zwischen Steuerungen . . . 105

Verwalten Ihrer Netzwerksicherheit

9 Systemstruktur 111
Aufbau der Systemstruktur . . . 111
Gruppe Eigenes Unternehmen . . . 112
Meine Gruppe . . . 112
Sammelgruppe . . . 112
Systemstrukturgruppen . . . 113
Vererbung . . . 113
Überlegungen beim Planen der Systemstruktur . . . 114
Administratorzugriff . . . 114
Gliederung der Umgebung und ihr Einfluss auf die Systemorganisation . . . 114
Subnetze und IP-Adressbereiche . . . 115
Betriebssysteme und Software . . . 115
Tags und Systeme mit ähnlichen Eigenschaften . . . 115
Active Directory-Synchronisierung . . . 116
Typen der Active Directory-Synchronisierung . . . 117
Systeme und Struktur . . . 117
Nur Systeme . . . 118
NT-Domänensynchronisierung . . . 118
Kriterienbasierte Sortierung . . . 118
Auswirkung von Einstellungen auf die Sortierung . . . 119
Kriterien für die IP-Adressensortierung . . . 120
Tag-basierte Sortierungskriterien . . . 120
Gruppenreihenfolge und -sortierung . . . 120
Erfassungsgruppen . . . 120
Hinzufügen eines Systems zur Systemstruktur bei aktivierter Sortierung . . . 121

Erstellen und Auffüllen von Systemstrukturgruppen . . . 122
Manuelles Erstellen von Gruppen . . . 123
Manuelles Hinzufügen von Systemen zu einer vorhandenen Gruppe . . . 124
Exportieren von Systemen aus der Systemstruktur . . . 124
Importieren von Systemen aus einer Textdatei . . . 125
Sortieren von Systemen in kriterienbasierten Gruppen . . . 126
Importieren von Active Directory-Containern . . . 129
Importieren von NT-Domänen in eine vorhandene Gruppe . . . 130
Planen der Systemstruktursynchronisierung . . . 132
Manuelles Aktualisieren einer synchronisierten Gruppe mit einer NT-Domäne . . . 133
Verschieben von Systemen innerhalb der Systemstruktur . . . 134
Funktionsweise von Systeme übertragen . . . 134
Übertragen von Systemen zwischen McAfee ePO-Servern . . . 135
Exportieren und Importieren von ASSC-Schlüsseln zwischen McAfee ePO-Servern . . . 136
Zusammenspiel der Funktion für automatische Antworten mit der Systemstruktur . . . 138
Beschränkung, Aggregation und Gruppierung . . . 138
Standardregeln . . . 139

10 Tags 141
Erstellen von Tags mit dem Tag-Generator . . . 141
Tags verwalten . . . 142
Erstellen, Löschen und Ändern von Tag-Untergruppen . . . 143
Ausschließen von Systemen von der automatischen Kennzeichnung . . . 144
Erstellen einer Abfrage zum Auflisten von Systemen anhand der Tags . . . 145
Anwenden von Tags auf ausgewählte Systeme . . . 146
Löschen eines Tags vom System . . . 147
Anwenden von kriterienbasierten Tags auf alle übereinstimmenden Systeme . . . 147
Planmäßiges Anwenden von kriterienbasierten Tags . . . 148

11 Agent-zu-Server-Kommunikation 149
Arbeiten mit dem Agenten auf dem McAfee ePO-Server . . . 149
Funktionsweise der Agent-zu-Server-Kommunikation . . . 149
SuperAgents und ihre Funktionsweise . . . 153
McAfee Agent-Relay-Funktionalität . . . 158
Peer-to-Peer-Kommunikation . . . 160
Erfassen von McAfee Agent-Statistiken . . . 162
Ändern der in der Benutzeroberfläche und dem Ereignisprotokoll des Agenten verwendeten Sprache . . . 162
Konfigurieren von ausgewählten Systemen für die Aktualisierung . . . 163
Antworten auf Richtlinienereignisse . . . 163
Planen von Client-Tasks . . . 164
Sofortiges Ausführen von Client-Tasks . . . 165
Ermitteln inaktiver Agenten . . . 166
Windows-Systeme und vom Agenten gemeldete Produkteigenschaften . . . 166
Von McAfee Agent bereitgestellte Abfragen . . . 168
Verwalten der Agenten-Server-Kommunikation . . . 169
Zulassen der Zwischenspeicherung von Anmeldeinformationen für die Agenten-Ausbringung . . . 169
Ändern der Ports für die Agenten-Kommunikation . . . 170

12 Sicherheitsschlüssel 171
Beschreibung und Funktionsweise von Sicherheitsschlüsseln . . . 171
Schlüsselpaar für Master-Repository . . . 172
Öffentliche Schlüssel für weitere Repositories . . . 172
Verwalten von Repository-Schlüsseln . . . 173
Verwenden eines Master-Repository-Schlüsselpaares für alle Server . . . 173

Verwenden von Schlüsseln für das Master-Repository in Umgebungen mit mehreren Servern . . . 174
ASSC-Schlüssel (Schlüssel für sichere Agenten-Server-Kommunikation) . . . 175
Verwalten von ASSC-Schlüsseln . . . 175
Anzeigen von Systemen, die ein ASSC-Schlüsselpaar verwenden . . . 177
Verwenden desselben ASSC-Schlüsselpaares für alle Server und Agenten . . . 177
Verwenden verschiedener ASSC-Schlüsselpaare für jeden McAfee ePO-Server . . . 178
Sichern und Wiederherstellen von Schlüsseln . . . 178

13 Software-Manager 181
Inhalt des Software-Managers . . . 181
Einchecken, Aktualisieren und Entfernen von Software mit dem Software-Manager . . . 182
Überprüfen der Produktkompatibilität . . . 183
Ändern der Einstellungen für den Download der Produktkompatibilitätsliste . . . 185

14 Produktausbringung 187
Auswählen einer Methode zur Produktausbringung . . . 187
Vorteile von Produktausbringungsprojekten . . . 188
Erklärung der Seite Produktausbringung . . . 190
Anzeigen von Audit-Protokollen zu Produktausbringungen . . . 191
Anzeigen der Produktausbringung . . . 191
Ausbringen von Produkten mithilfe eines Ausbringungsprojekts . . . 192
Überwachen und Bearbeiten von Ausbringungsprojekten . . . 194
Beispiel für die Bereitstellung eines neuen Produkts . . . 195
Globale Aktualisierung . . . 196
Automatisches Ausbringen von Aktualisierungspaketen per globaler Aktualisierung . . . 198

15 Manuelle Verwaltung von Paketen und Aktualisierungen 199
Hinzufügen von Produkten zur Verwaltung . . . 199
Manuelles Einchecken von Paketen . . . 200
Löschen von DAT- oder Scan-Modul-Paketen aus dem Master-Repository . . . 200
Manuelles Verschieben von DAT- und Scan-Modul-Paketen zwischen Zweigen . . . 201
Manuelles Einchecken von Scan-Modul-, DAT- und EXTRA.DAT-Aktualisierungspaketen . . . 201

16 Richtlinienverwaltung 203
Richtlinien und Richtlinienerzwingung . . . 203
Richtlinienanwendung . . . 205
Erstellen und Verwalten von Richtlinien . . . 206
Erstellen einer Richtlinie auf der Seite Richtlinienkatalog . . . 206
Verwalten einer vorhandenen Richtlinie auf der Seite Richtlinienkatalog . . . 207
Erstmaliges Konfigurieren von Richtlinien . . . 208
Verwalten von Richtlinien . . . 208
Ändern der Besitzer einer Richtlinie . . . 209
Verschieben von Richtlinien zwischen McAfee ePO-Servern . . . 210
Zuweisen einer Richtlinie zu einer Systemstrukturgruppe . . . 211
Zuweisen einer Richtlinie zu einem verwalteten System . . . 211
Zuweisen einer Richtlinie zu Systemen in einer Systemstrukturgruppe . . . 212
Erzwingen von Richtlinien für ein Produkt in einer Systemstrukturgruppe . . . 212
Erzwingen von Richtlinien für ein Produkt auf einem System . . . 213
Kopieren von Richtlinienzuweisungen . . . 213
Aufbewahrung von Richtlinien und Tasks: Bearbeiten, Seite . . . 215
Richtlinienzuweisungsregeln . . . 216
Priorität von Richtlinienzuweisungsregeln . . . 216
Benutzerbasierte Richtlinienzuweisungen . . . 217
Informationen zu systembasierten Richtlinienzuweisungen . . . 218
Zuweisen von systembasierten Richtlinien mithilfe von Tags . . . 218

Erstellen von Richtlinienzuweisungsregeln . . . 218
Verwalten von Richtlinienzuweisungsregeln . . . 219
Erstellen von Abfragen zur Richtlinienverwaltung . . . 220
Erstellen einer Abfrage zum Definieren der Compliance . . . 221
Generieren von Compliance-Ereignissen . . . 222
Anzeigen der Richtlinieninformationen . . . 223
Anzeigen der Gruppen und Systeme, denen eine Richtlinie zugewiesen ist . . . 223
Anzeigen von Richtlinieneinstellungen . . . 224
Anzeigen des Richtlinienbesitzes . . . 224
Anzeigen von Zuweisungen, bei denen die Richtlinienerzwingung deaktiviert ist . . . 224
Anzeigen der einer Gruppe zugewiesenen Richtlinien . . . 225
Anzeigen der einem bestimmten System zugewiesenen Richtlinien . . . 225
Anzeigen der Richtlinienvererbung für eine Gruppe . . . 225
Anzeigen und Zurücksetzen einer unterbrochenen Vererbung . . . 226
Vergleichen von Richtlinien . . . 226
Freigeben von Richtlinien zwischen McAfee ePO-Servern . . . 227
Verteilen einer Richtlinie an mehrere McAfee ePO-Server . . . 227
Registrieren von Servern zur Richtlinienfreigabe . . . 227
Bestimmen von Richtlinien zur Freigabe . . . 227
Planen von Server-Tasks zum Freigeben von Richtlinien . . . 228
Fragen zur Richtlinienverwaltung . . . 228

17 Client-Tasks 231
Funktionsweise des Client-Task-Katalogs . . . 231
Ausbringungs-Tasks . . . 232
Ausbringungspakete für Produkte und Aktualisierungen . . . 232
Ausbringen von Produkten und Aktualisierungen . . . 234
Erstmaliges Konfigurieren der Ausbringungen von Produkten und Aktualisierungen . . . 234
Bereitstellungs-Tags . . . 235
Ausbringen von Produkten auf verwaltete Systeme mithilfe des Produktausbringungs-Tasks . . . 235
Konfigurieren eines Ausbringungs-Tasks für Gruppen verwalteter Systeme . . . 235
Konfigurieren eines Ausbringungs-Tasks zum Installieren von Produkten auf einem verwalteten System . . . 237
Aktualisierungs-Tasks . . . 238
Anzeigen eines zugewiesenen Client-Tasks . . . 239
Regelmäßiges Aktualisieren von verwalteten Systemen mit einem geplanten Aktualisierungs-Task . . . 239
Testen neuer DAT-Dateien und Scan-Module vor dem Verteilen . . . 240
Verwalten von Client-Tasks . . . 241
Erstellen von Client-Tasks . . . 241
Bearbeiten von Client-Tasks . . . 242
Löschen von Client-Tasks . . . 242
Vergleichen von Client-Tasks . . . 243

18 Server-Tasks 245
Erstellen eines Server-Tasks . . . 245
Zulässige Cron-Syntax beim Planen von Server-Tasks . . . 246
Das Server-Task-Protokoll . . . 247
Anzeigen von Informationen zu Server-Tasks im Server-Task-Protokoll . . . 247
Verwalten des Server-Task-Protokolls . . . 247

19 Verwalten von SQL-Datenbanken 249
Warten von SQL-Datenbanken . . . 249
Ermitteln des Servers und des Namens der Microsoft SQL-Datenbank mithilfe eines Remote-Befehls . . . 249
Konfigurieren eines Snapshots und Wiederherstellen der SQL-Datenbank . . . 250

Konfigurieren eines Tasks zur Erstellung eines Server-Snapshots für die Wiederherstellung nach einem Systemausfall . . . 250
Sichern und Wiederherstellen von Datenbanken mithilfe von Microsoft SQL Server . . . 251
Ermitteln des Servers und des Namens der Microsoft SQL-Datenbank mithilfe eines Remote-Befehls . . . 252
Ermitteln von Informationen über den McAfee ePO-Server mithilfe von Microsoft SQL Server Management Studio . . . 252
Das Bedrohungsereignisprotokoll . . . 253
Anzeigen und Bereinigen des Bedrohungsereignisprotokolls . . . 254
Planen der Bereinigung des Bedrohungsereignisprotokolls . . . 255

Überwachung und Berichterstellung zum Netzwerk-Sicherheitsstatus

20 Dashboards und Monitore 259
Verwenden von Dashboards und Monitoren . . . 259
Verwalten von Dashboards . . . 260
Exportieren und Importieren von Dashboards . . . 262
Verwalten von Dashboard-Monitoren . . . 263
Verschieben und Ändern der Größe von Dashboard-Monitoren . . . 265
Standard-Dashboards und deren Monitore . . . 265
Festlegen von ersten Dashboards und Dashboard-Aktualisierungsintervallen . . . 267

21 Abfragen und Berichte 269
Berechtigungen für Abfragen und Berichte . . . 269
Informationen zu Abfragen . . . 270
Abfragen-Generator . . . 271
Erstmaliges Konfigurieren von Abfragen und Berichten . . . 272
Arbeiten mit Abfragen . . . 272
Verwalten benutzerdefinierter Abfragen . . . 273
Ausführen einer Abfrage . . . 275
Planmäßiges Ausführen einer Abfrage . . . 275
Erstellen einer Abfragegruppe . . . 276
Verschieben einer Abfrage in eine andere Gruppe . . . 277
Exportieren und Importieren von Abfragen . . . 277
Exportieren von Abfrageergebnissen in andere Formate . . . 278
Zusammengefasste Abfragen mehrerer Server . . . 279
Erstellen eines Server-Tasks zum Zusammenfassen von Daten . . . 280
Informationen zu Berichten . . . 281
Struktur von Berichten . . . 281
Arbeiten mit Berichten . . . 282
Erstellen eines Berichts . . . 283
Bearbeiten eines vorhandenen Berichts . . . 283
Anzeigen von Berichtergebnissen . . . 288
Gruppieren von Berichten . . . 288
Ausführen von Berichten . . . 289
Planmäßiges Ausführen eines Berichts . . . 289
Exportieren und Importieren von Berichten . . . 290
Konfigurieren der Vorlage und des Speicherorts für exportierte Berichte . . . 291
Löschen von Berichten . . . 292

22 Ereignisse und Antworten 293
Verwenden automatischer Antworten . . . 293
Beschränkung, Aggregation und Gruppierung . . . 294
Standardregeln . . . 294
Planen von Antworten . . . 295

Erstmaliges Konfigurieren von Antworten . . . 296
Bestimmen, wie Ereignisse weitergeleitet werden . . . 296
Bestimmen der sofort weiterzuleitenden Ereignisse . . . 297
Bestimmen der weiterzuleitenden Ereignisse . . . 297
Konfigurieren automatischer Antworten . . . 298
Zuweisen von Berechtigungen für Benachrichtigungen . . . 298
Zuweisen von Berechtigungen für automatische Antworten . . . 299
Verwalten von SNMP-Servern . . . 299
Bestimmen der an den Server weiterzuleitenden Ereignisse . . . 302
Auswählen eines Intervalls für Benachrichtigungsereignisse . . . 302
Erstellen und Bearbeiten von Regeln für automatische Antworten . . . 303
Beschreiben einer Regel . . . 303
Festlegen von Filtern für die Regel . . . 303
Festlegen von Schwellenwerten für die Regel . . . 304
Konfigurieren der Aktion für Regeln zu automatischen Antworten . . . 304
Fragen zu Ereignissen und Antworten . . . 306

23 Probleme 307
Beschreibung und Funktionsweise von Problemen . . . 307
Arbeiten mit Problemen . . . 307
Manuelles Erstellen von einfachen Problemen . . . 308
Konfigurieren von Antworten zum automatischen Erstellen von Problemen . . . 309
Verwalten von Problemen . . . 309
Bereinigen abgeschlossener Probleme . . . 310
Manuelles Bereinigen abgeschlossener Probleme . . . 310
Planmäßiges Bereinigen abgeschlossener Probleme . . . 311

24 Wiederherstellung nach Systemausfall 313
Was ist eine Wiederherstellung nach einem Systemausfall? . . . 313
Komponenten für die Wiederherstellung nach einem Systemausfall . . . 314
Funktionsweise der Wiederherstellung nach einem Systemausfall . . . 317
Überblick über Snapshots zur Wiederherstellung nach einem Systemausfall und Sicherungen . . . 317
McAfee ePO Überblick über eine Wiederherstellungsinstallation . . . 319
Erstellen eines Snapshots . . . 321
Erstellen von Snapshots im Dashboard . . . 321
Erstellen von Snapshots per Web-API . . . 322
Konfigurieren von Server-Einstellungen zur Wiederherstellung nach einem Systemausfall . . . 324

A Ports – Übersicht 327
Ändern des Konsolen-Ports zur Anwendungs-Server-Kommunikation . . . 327
Ändern des Ports für Agent-Server-Kommunikation . . . 329
Erforderliche Ports für die Kommunikation durch eine Firewall . . . 332
Datenverkehr – Kurzanleitung . . . 333

B Öffnen einer remoten Konsolenverbindung 335

Index 337

Einleitung

In diesem Handbuch finden Sie die erforderlichen Informationen für die Arbeit mit Ihrem McAfee-Produkt.

Inhalt

- *Informationen zu diesem Handbuch*
- *Quellen für Produktinformationen*

Informationen zu diesem Handbuch

In diesem Abschnitt werden die Zielgruppe des Handbuchs, die verwendeten typografischen Konventionen und Symbole sowie die Gliederung des Handbuchs beschrieben.

Zielgruppe

Die Dokumentation von McAfee wird inhaltlich sorgfältig auf die Zielgruppe abgestimmt.

Die Informationen in diesem Handbuch richten sich in erster Linie an:

- **Administratoren** – Personen, die das Sicherheitsprogramm eines Unternehmens implementieren und umsetzen.
- **Benutzer** – Personen, die den Computer verwenden, auf dem die Software ausgeführt wird, und die auf einige oder alle Funktionen zugreifen können.

Konventionen

In diesem Handbuch werden folgende typografische Konventionen und Symbole verwendet.

Buchtitel, *Begriff*, *Hervorhebung*	Titel eines Buchs, Kapitels oder Themas; ein neuer Begriff; eine Hervorhebung.
Fett	Text, der stark hervorgehoben wird.
`Benutzereingabe, Code, Meldung`	Befehle oder andere Texte, die vom Benutzer eingegeben werden; ein Code-Beispiel; eine angezeigte Meldung.
Benutzeroberflächentext	Wörter aus der Benutzeroberfläche des Produkts, z. B. Optionen, Menüs, Schaltflächen und Dialogfelder.
Hypertext-Blau	Ein Link auf ein Thema oder eine externe Website.
	Hinweis: Zusätzliche Informationen, beispielsweise eine alternative Methode für den Zugriff auf eine Option.
	Tipp: Vorschläge und Empfehlungen.

Wichtig/Vorsicht: Wichtige Ratschläge zum Schutz Ihres Computersystems, der Software-Installation, des Netzwerks, Ihres Unternehmens oder Ihrer Daten.

Warnung: Wichtige Ratschläge, um körperliche Verletzungen bei der Nutzung eines Hardware-Produkts zu vermeiden.

Quellen für Produktinformationen

Nach der Veröffentlichung eines Produkts werden Informationen zu dem Produkt im Online-Knowledge Center von McAfee eingegeben.

Vorgehensweise

1. Rufen Sie das McAfee ServicePortal unter http://support.mcafee.com auf, und klicken Sie auf **Knowledge Center**.
2. Geben Sie einen Produktnamen ein, wählen Sie eine Version, und klicken Sie dann auf **Suchen**, um eine Liste der Dokumente anzuzeigen.

Einführung in McAfee ePolicy Orchestrator

Kapitel 1 *Schützen Ihrer Netzwerke mithilfe von ePolicy Orchestrator*
Kapitel 2 *Verwenden der ePolicy Orchestrator-Benutzeroberfläche*

1 Schützen Ihrer Netzwerke mithilfe von ePolicy Orchestrator

ePolicy Orchestrator ist eine zentrale Komponente der McAfee-Sicherheitsverwaltungsplattform, mit der Sie die Sicherheit von Endgeräten, Netzwerken und Daten einheitlich verwalten können. Durch die Automatisierungsfunktionen von ePolicy Orchestrator und durchgängige Netzwerktransparenz werden Reaktionszeiten verkürzt, der Schutz verbessert und die Risiko- sowie Sicherheitsverwaltung vereinfacht.

Inhalt

- *Vorteile von ePolicy Orchestrator*
- *Komponenten und ihre Funktion*
- *Funktionsweise der Software*

Vorteile von ePolicy Orchestrator

ePolicy Orchestrator ist eine erweiterbare Verwaltungsplattform, die eine zentralisierte Richtlinienverwaltung und -erzwingung von Sicherheitsrichtlinien ermöglicht.

Mit ePolicy Orchestrator können Sie die folgenden Aufgaben im Zusammenhang mit der Netzwerksicherheit ausführen:

- Sie können Richtlinienzuweisungen und Client-Tasks im Zusammenhang mit der Netzwerksicherheit verwalten und erzwingen.
- Sie können die von Ihrer Sicherheits-Software benötigten Virusdefinitionsdateien (DAT-Dateien), Virenschutz-Module und anderen Sicherheitsinhalte aktualisieren, um die Sicherheit Ihrer verwalteten Systeme zu gewährleisten.
- Erstellen von Berichten mithilfe des integrierten Abfragesystem-Assistenten, die informative vom Benutzer konfigurierte Diagramme und Tabellen mit den Daten zu Ihrer Netzwerksicherheit enthalten.

Komponenten und ihre Funktion

Die ePolicy Orchestrator-Software besteht aus den folgenden Komponenten.

- **McAfee ePO-Server**: Der Mittelpunkt einer verwalteten Umgebung. Über den Server werden Sicherheitsrichtlinien und Tasks bereitgestellt, Aktualisierungen gesteuert und Ereignisse für alle verwalteten Systeme verarbeitet.
- **Datenbank**: Die zentrale Speicherkomponente für alle von ePolicy Orchestrator erstellten und verwendeten Daten. Sie können je nach den Anforderungen des Unternehmens selbst auswählen, ob sich die Datenbank auf dem McAfee ePO-Server oder auf einem separaten System befinden soll.

- **McAfee Agent** : Ein Hilfsmittel zum Übertragen von Informationen und zum Erzwingen von Richtlinien zwischen dem McAfee ePO-Server und den einzelnen verwalteten Systemen. Über den Agenten werden für jedes verwaltete System Aktualisierungen abgerufen, die Implementierung von Tasks sichergestellt, Richtlinien erzwungen und Ereignisse weitergeleitet. Die Daten werden über einen separaten sicheren Datenkanal an den Server übertragen. McAfee Agent kann auch als SuperAgent konfiguriert werden.
- **Master-Repository**: Der zentrale Speicherort für alle McAfee-Aktualisierungen und -Signaturen auf dem McAfee ePO-Server. Im Master-Repository werden vom Benutzer angegebene Aktualisierungen und Signaturen von McAfee oder von benutzerdefinierten Quellsites abgerufen.
- **Verteilte Repositories**: Strategisch günstig über die gesamte Umgebung verteilte lokale Zugriffspunkte, von denen Agenten Signaturen, Produktaktualisierungen und Produktinstallationen bei minimaler Auswirkung auf die Bandbreite empfangen können. Je nach Konfiguration des Netzwerks können Sie verteilte Repositories für SuperAgent oder für die HTTP-, FTP- bzw. UNC-Freigabe einrichten.
- **Remote-Agentensteuerungen**: Ein Server, den Sie zur Unterstützung beim Verwalten der Agenten-Kommunikation, beim Lastausgleich und bei Produktaktualisierungen an verschiedenen Stellen im Netzwerk installieren können. Remote-Agentensteuerungen bestehen aus einem Apache-Server und einer Ereignisanalyse. Mit ihrer Hilfe können Sie die Anforderungen großer oder komplexer Netzwerkinfrastrukturen besser bewältigen, da sie eine bessere Kontrolle über die Agent-Server-Kommunikation ermöglichen.
- **Registrierte Server**: Werden verwendet, um andere Server bei Ihrem McAfee ePO-Server zu registrieren. Zu den Typen registrierter Server gehören:
  - **LDAP-Server**: Wird für Richtlinienzuweisungsregeln sowie zum Aktivieren der automatischen Benutzerkontenerstellung verwendet.
  - **SNMP-Server**: Wird zum Empfangen eines SNMP-Traps verwendet. Fügen Sie die Informationen für den SNMP-Server hinzu, damit das Ziel des Traps in ePolicy Orchestrator klar angegeben ist.
  - **Datenbank-Server**: Wird verwendet, um die Tools zur erweiterten Berichterstellung aus dem Lieferumfang der ePolicy Orchestrator-Software zu erweitern.

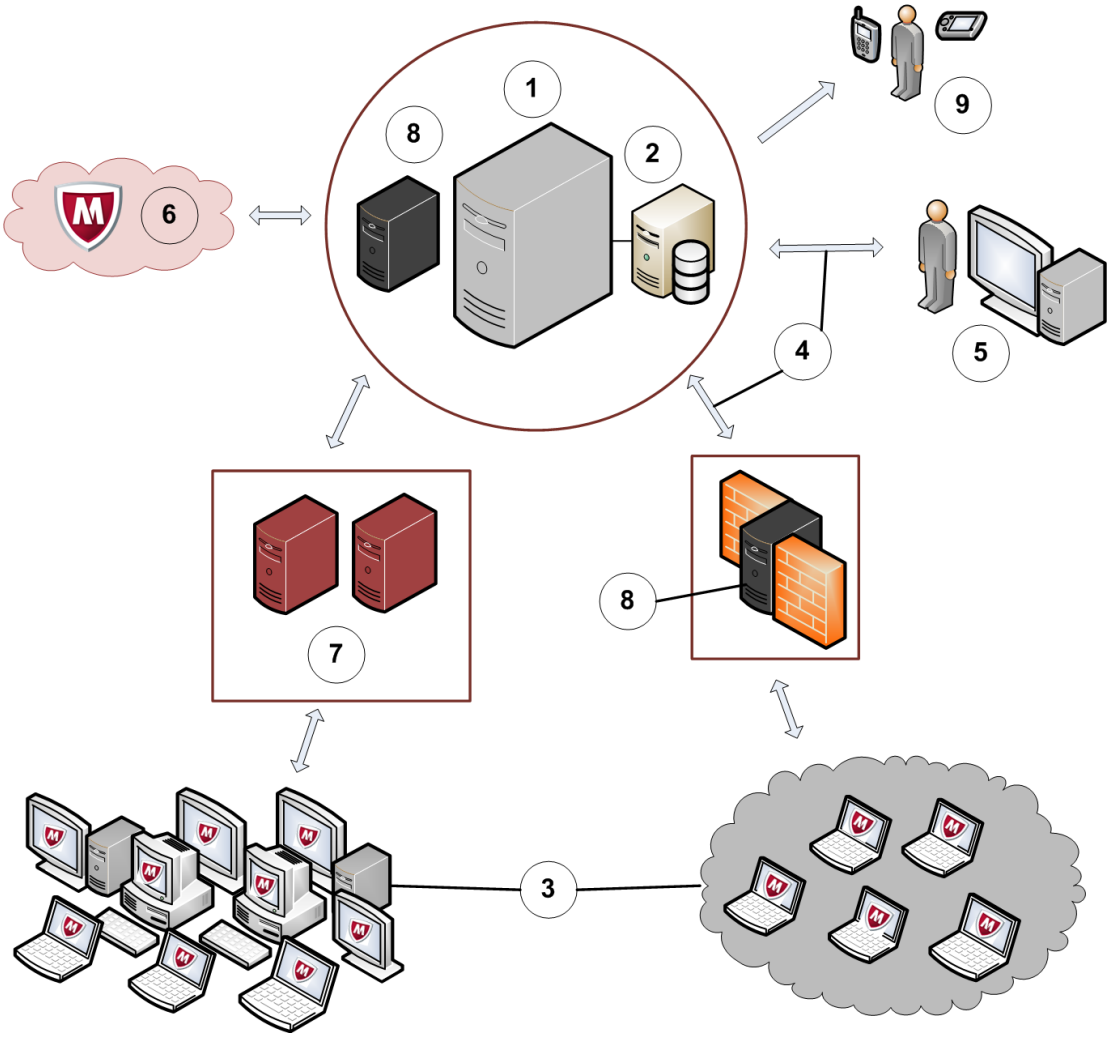
Je nach den Anforderungen des Unternehmens und der Komplexität des Netzwerks sind möglicherweise nicht alle diese Komponenten erforderlich.

Funktionsweise der Software

ePolicy Orchestrator ist äußerst flexibel. Die Software kann auf verschiedene Weisen eingerichtet werden, um Ihre Anforderungen zu erfüllen.

Die Software folgt dem klassischen Client-Server-Modell, bei dem ein Client-System (System) Anweisungen vom Server erhält. Um diesen Kontakt zum Server zu ermöglichen, wird auf jedem System im Netzwerk eine Instanz von McAfee Agent ausgebracht. Sobald ein Agent auf einem System ausgebracht ist, kann das System von McAfee ePO-Server verwaltet werden. Die sichere Kommunikation zwischen dem Server und dem verwalteten System ist das Bindeglied, das sämtliche

Komponenten von ePolicy Orchestrator miteinander verknüpft. In der folgenden Abbildung wird anhand eines Beispiels gezeigt, wie der McAfee ePO-Server und seine Komponenten in einer sicheren Netzwerkumgebung miteinander interagieren.



1 Der McAfee ePO-Server ist mit dem McAfee-Aktualisierungs-Server verbunden, um aktuelle Sicherheitsinhalte abzurufen.

2 In der ePolicy Orchestrator-Datenbank werden sämtliche Daten zu den im Netzwerk verwalteten Systemen gespeichert. Dazu gehören:

- Systemeigenschaften
- Richtlinieninformationen
- Verzeichnisstruktur
- Alle sonstigen relevanten Daten, die der Server benötigt, um die Systeme auf dem aktuellen Stand zu halten

3 Auf den Systemen ist McAfee Agent bereitgestellt, um Folgendes zu ermöglichen:

- Richtlinienerzwingung
- Produktausbringungen und -aktualisierungen
- Berichterstellung zu den verwalteten Systemen

4 In regelmäßigen Abständen erfolgt zwischen den Systemen und dem Server eine sichere Agenten-Server-Kommunikation (ASSC). Wenn im Netzwerk remote Agentensteuerungen installiert sind, kommunizieren die Agenten über die ihnen zugewiesenen Agentensteuerungen mit dem Server.

5 Benutzer melden sich bei der ePolicy Orchestrator-Konsole an, um Sicherheitsverwaltungsaufgaben durchzuführen (z. B. Ausführen von Abfragen, um Berichte zum Sicherheitsstatus zu erstellen, oder Arbeiten mit den Sicherheitsrichtlinien von verwalteten Produkten).

6 Auf dem McAfee-Aktualisierungs-Server befinden sich die aktuellsten Sicherheitsinhalte, von wo sie ePolicy Orchestrator in geplanten Abständen abrufen kann.

7 Im gesamten Netzwerk platzierte verteilte Repositories dienen als lokale Hosts für Sicherheitsinhalte, damit Agenten ihre Aktualisierungen schneller erhalten.

8 Mithilfe von Remote-Agentensteuerungen können Sie das Netzwerk leichter skalieren, um mit einem einzigen McAfee ePO-Server mehr Agenten zu verwalten.

9 Benachrichtigungen vom Typ "Automatische Antwort" werden an Sicherheitsadministratoren gesendet, um sie beim Auftreten bestimmter Ereignisse zu informieren.

2 Verwenden der ePolicy Orchestrator-Benutzeroberfläche

Melden Sie sich bei der ePolicy Orchestrator-Benutzeroberfläche an, um den McAfee ePO-Server zu konfigurieren und die Netzwerksicherheit zu verwalten und zu überwachen.

Inhalt

- *Anmelden und Abmelden*
- *Navigieren in der Benutzeroberfläche*
- *Arbeiten mit Listen und Tabellen*

Anmelden und Abmelden

Geben Sie auf dem Anmeldebildschirm den Benutzernamen und das Kennwort ein, um auf die ePolicy Orchestrator-Software zuzugreifen.

Bevor Sie beginnen

Sie benötigen für die Anmeldung bei ePolicy Orchestrator einen Benutzernamen und ein Kennwort.

Unabhängig davon, ob Sie die Verbindung mit dem McAfee ePO-Server über eine Remote-Verbindung oder über das McAfee ePO-Serversymbol herstellen, wird als erster Bildschirm der ePolicy Orchestrator-Anmeldebildschirm angezeigt.

Vorgehensweise

1. Geben Sie den Benutzernamen und das Kennwort ein, und klicken Sie auf **Anmelden**.

   In der ePolicy Orchestrator-Software wird das Standard-Dashboard angezeigt.

2. Zum Beenden der ePolicy Orchestrator-Sitzung klicken Sie auf **Abmelden**.

Nach der Abmeldung wird die Sitzung geschlossen und kann nicht von anderen Benutzern geöffnet werden.

Navigieren in der Benutzeroberfläche

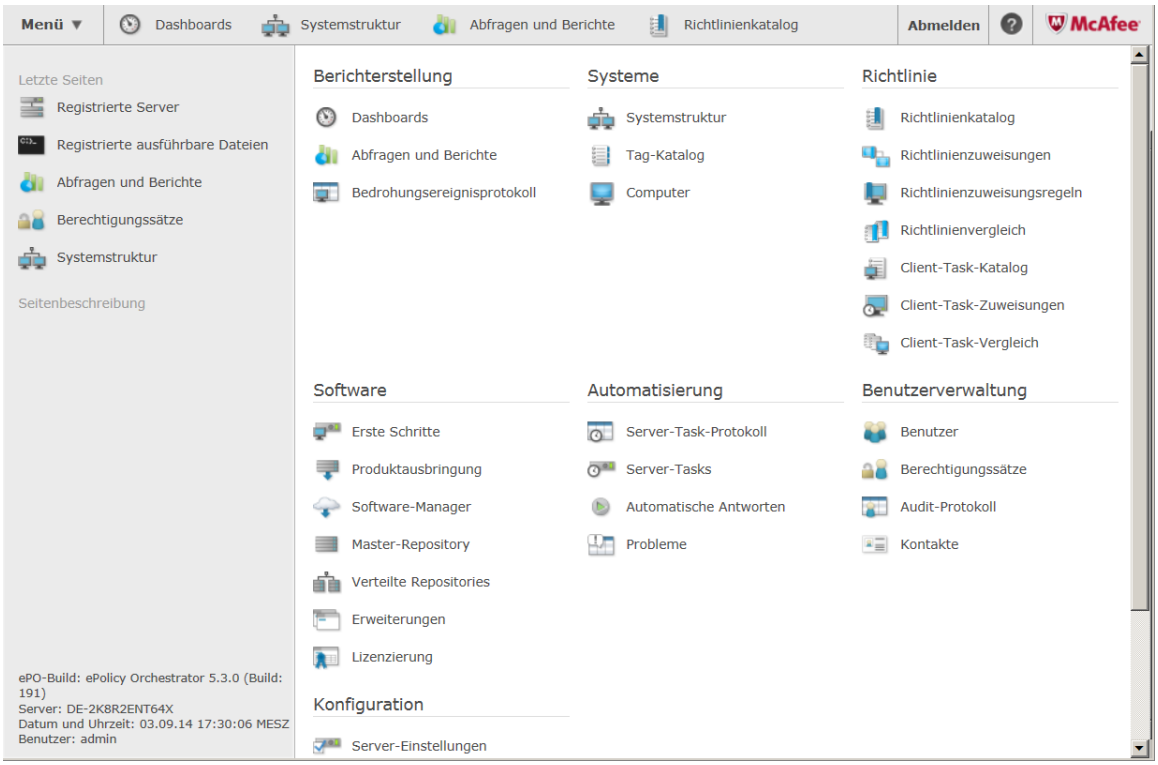
Auf der Benutzeroberfläche von McAfee ePO wird eine menübasierte Navigation mit einer anpassbaren Favoritenleiste verwendet, sodass Sie schnell zu den gewünschten Bereichen gelangen.

Die Menüabschnitte entsprechen den wichtigsten Funktionen. Wenn Sie verwaltete Produkte zu McAfee ePO hinzufügen, nimmt die Zahl der Menüoptionen zu.

Verwenden des ePolicy Orchestrator-Navigationsmenüs

Öffnen Sie das ePolicy Orchestrator-Menü, um auf der Benutzeroberfläche von ePolicy Orchestrator zu navigieren.

Das Menü besteht aus Kategorien, in denen die verschiedenen Funktionen und Merkmale von McAfee ePO enthalten sind. Jede Kategorie enthält eine Liste der Seiten für die wichtigsten Funktionen, die mit einem eindeutigen Symbol versehen sind. Wählen Sie eine Kategorie im Menü aus, um die Hauptseiten der entsprechenden Funktion anzuzeigen.



Anpassen der Navigationsleiste

Die Navigationsleiste kann angepasst werden, um einen schnellen Zugriff auf die am häufigsten genutzten Funktionen und Merkmale zu ermöglichen.

Sie können selbst entscheiden, welche Symbole in der Navigationsleiste angezeigt werden, indem Sie beliebige Menüelemente in die Navigationsleiste ziehen oder daraus wieder entfernen.

Wenn Sie mehr Symbole in der Navigationsleiste platzieren, als angezeigt werden können, wird auf der rechten Seite der Leiste ein Einblendmenü erstellt. Klicken Sie auf das Pfeilsymbol, um auf die Menüelemente zuzugreifen, die nicht in der Navigationsleiste angezeigt werden. Die in der Navigationsleiste angezeigten Symbole werden als Einstellungen des jeweiligen Benutzers gespeichert. Jedem Benutzer wird also unabhängig von der Konsole, an der er sich anmeldet, seine angepasste Navigationsleiste angezeigt.

Server-Einstellungskategorien

Diese standardmäßigen Server-Einstellungskategorien stehen in McAfee ePO zur Verfügung.

Beim Hinzufügen weiterer Software zum McAfee ePO-Server werden produktspezifische Server-Einstellungen zur Liste der Server-Einstellungskategorien hinzugefügt. Server-Einstellungen

können Sie auf der Seite Server-Einstellungen im Abschnitt Konfiguration der Benutzeroberfläche von McAfee ePO ändern.

Informationen zu produktspezifischen Server-Einstellungen finden Sie in der zugehörigen Produktdokumentation.

Tabelle 2-1 Kategorien von standardmäßigen Server-Einstellungen und deren Beschreibungen

Server-Einstellungskategorie	Beschreibung
Active Directory-Gruppen	Gibt für jede Domäne den zu verwendenden LDAP-Server an.
Active Directory-Benutzeranmeldung	Gibt an, ob sich Mitglieder zugeordneter Active Directory-Gruppen (AD) mit ihren AD-Anmeldeinformationen beim Server anmelden können, sobald die Funktion Active Directory-Benutzeranmeldung vollständig konfiguriert ist.
Methode für Agentenkontakt	Legt fest, mit welcher Priorität von McAfee ePO Methoden verwendet werden, um Kontakt mit McAfee Agent aufzunehmen. Zum Ändern der Priorität wählen Sie unter **Einstellungskategorien** die Option **Methode für Agentenkontakt** aus, klicken Sie auf **Bearbeiten**, und wählen Sie dann die Priorität aus. Für jede Kontaktmethode muss eine andere Prioritätsstufe festgelegt werden. Für die Kontaktaufnahme mit McAfee Agent sind folgende Methoden verfügbar: • **Vollqualifizierter Domänenname** • **NetBIOS-Name** • **IP-Adresse**
Anmeldeinformationen für Agentenbereitstellung	Gibt an, ob Benutzer die Anmeldeinformationen für die Agentenbereitstellung im Cache ablegen dürfen.
Zertifikatbasierte Authentifizierung	Gibt an, ob Zertifikatbasierte Authentifizierung aktiviert ist und welche Einstellungen und Konfigurationen für das verwendete Zertifizierungsstellen-Zertifikat erforderlich sind.
Dashboards	Gibt das standardmäßig aktive Dashboard an, das dem Konto eines neues Benutzers zum Zeitpunkt der Erstellung zugewiesen wird, sowie die standardmäßige Aktualisierungsrate (fünf Minuten) für Dashboard-Monitore.
Wiederherstellung nach Systemausfall	Legt die Passphrase für die Schlüsselspeicherverschlüsselung zur Wiederherstellung nach einem Systemausfall fest und aktiviert sie.
E-Mail-Server	Gibt den E-Mail-Server an, über den E-Mail-Nachrichten von McAfee ePO gesendet werden.
Ereignisfilterung	Gibt an, welche Ereignisse vom Agenten weitergeleitet werden.
Ereignisbenachrichtigungen	Gibt an, wie oft die Benachrichtigungen von McAfee ePO daraufhin überprüft werden, ob automatische Reaktionen ausgelöst werden.
Globale Aktualisierung	Gibt an, ob und wie die globale Aktualisierung aktiviert ist.
Lizenzschlüssel	Gibt den Lizenzschlüssel an, mit dem diese McAfee ePO-Software registriert wurde.
Anmeldenachricht	Gibt an, ob eine benutzerdefinierte Nachricht angezeigt wird, wenn sich Benutzer bei der McAfee ePO-Konsole anmelden, und legt den Inhalt der Nachricht fest.
Aufbewahrung von Richtlinien und Tasks	Gibt an, ob Richtlinien und Client-Task-Daten entfernt werden, wenn Sie die Produkterweiterung löschen.

Tabelle 2-1 Kategorien von standardmäßigen Server-Einstellungen und deren Beschreibungen *(Fortsetzung)*

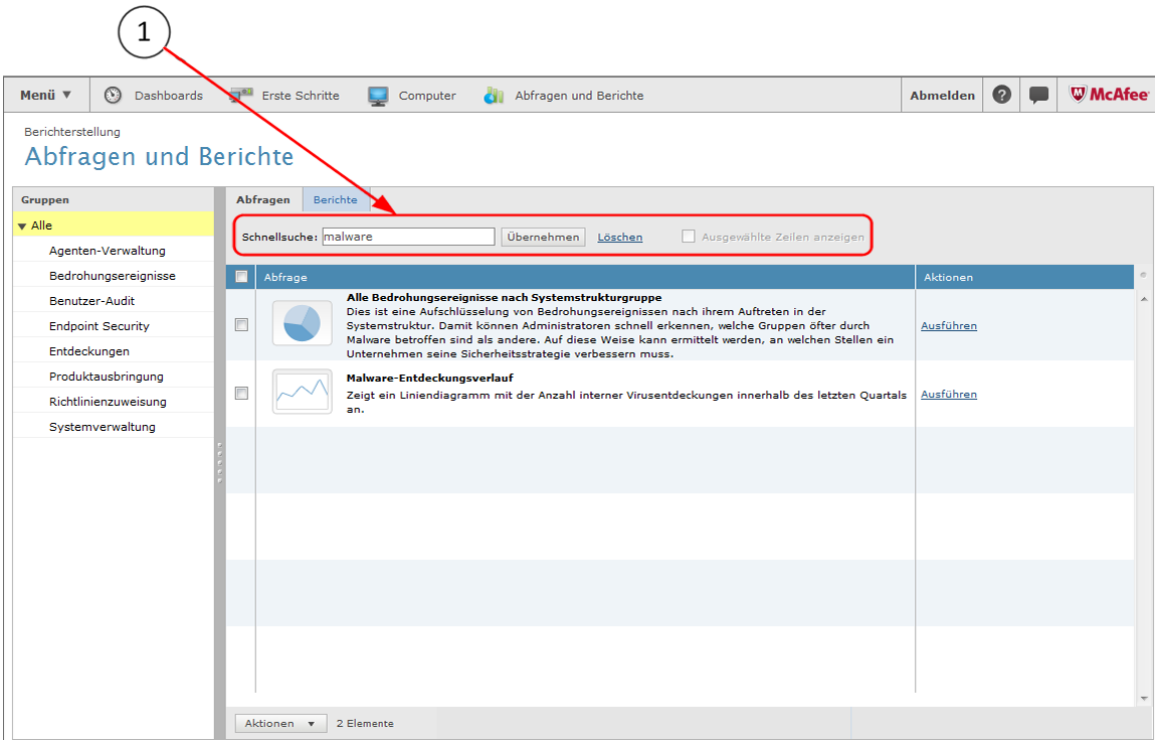
Server-Einstellungskategorie	Beschreibung
Richtlinienwartung	Gibt an, ob Richtlinien für nicht unterstützte Produkte ein- oder ausgeblendet werden. Dies ist nur erforderlich, wenn ein Upgrade für McAfee ePO von einer vorherigen Version durchgeführt wurde.
Ports	Gibt die Ports an, die vom Server für die Kommunikation mit Agenten und der Datenbank verwendet werden.
Drucken und exportieren	Gibt an, wie Informationen in andere Formate exportiert werden, und welche Vorlage bei PDF-Exporten verwendet wird. Außerdem gibt diese Einstellung den Standardspeicherort für die exportierten Dateien an.
Produktkompatibilitätsliste	Gibt an, ob die Produktkompatibilitätsliste automatisch heruntergeladen wird und nicht kompatible Produkterweiterungen angezeigt werden.
Product Improvement Program	Gibt an, ob von McAfee ePO proaktiv und in regelmäßigen Abständen Daten von den verwalteten Client-Systemen erfasst werden dürfen.
Proxy-Einstellungen	Gibt den Typ der für den McAfee ePO-Server konfigurierten Proxy-Einstellungen an.
Server-Informationen	Gibt Server-Informationen für Java, OpenSSL und Apache an, beispielsweise Name, IP-Adresse und Versionsinformationen.
Sicherheitsschlüssel	Gibt die Schlüssel für sichere Agenten-Server-Kommunikation und Repository-Schlüssel an und verwaltet sie.
Server-Zertifikat	Gibt das Server-Zertifikat an, das vom McAfee ePO-Server bei der HTTPS-Kommunikation mit Browsern verwendet wird.
Software-Test	Gibt die erforderlichen Informationen für das Einchecken und Bereitstellen von Test-Software im Software-Manager an.
Quellsites	Gibt die Quellsites an, mit denen vom Server für Aktualisierungen eine Verbindung hergestellt wird, sowie die Sites, die als alternative Sites verwendet werden sollen.
Systemdetaileinstellungen	Gibt an, welche Abfragen und Systemeigenschaften auf der Seite Systemdetails für verwaltete Systeme angezeigt werden.
Systemstruktursortierung	Gibt an, ob und wie die Systemstruktursortierung in der Umgebung aktiviert ist.
Benutzersitzung	Gibt an, wie lange Benutzer inaktiv sein dürfen, bevor sie vom System abgemeldet werden.

Arbeiten mit Listen und Tabellen

Verwenden Sie die ePolicy Orchestrator-Funktionen zur Suche und Filterung, um Datenlisten zu sortieren.

Datenlisten in ePolicy Orchestrator können Hunderte oder Tausende Einträge enthalten. Manuell nach bestimmten Einträgen in diesen ePolicy Orchestrator-Listen zu suchen, kann ohne den Suchfilter Schnellsuche schwierig sein.

Die Zahl in dieser Abbildung zeigt die Suchfilterung der Schnellsuche für Abfragen an, die die Zeichenfolge `malware` enthalten.



Filtern einer Liste

Sie können voreingestellte oder benutzerdefinierte Filter verwenden, um bestimmte Zeilen in den Datenlisten der ePolicy Orchestrator-Oberfläche auszuwählen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Leiste oberhalb der Liste den voreingestellten oder benutzerdefinierten Filter aus, mit dem die Liste gefiltert werden soll.

   Es werden nur Einträge angezeigt, die den Filterkriterien entsprechen.

2 Aktivieren Sie die Kontrollkästchen neben den Listeneinträgen, auf die Sie sich konzentrieren möchten, und wählen Sie dann **Ausgewählte Zeilen anzeigen** aus.

   Es werden nur die ausgewählten Zeilen angezeigt.

Suchen nach bestimmten Listeneinträgen

Verwenden Sie den Filter Schnellsuche, um Einträge in einer längeren Liste schneller zu finden.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Geben Sie Ihren Suchbegriff in das Feld **Schnellsuche** ein.

2 Klicken Sie auf **Übernehmen**.

Es werden nur die Elemente angezeigt, die die im Feld **Schnellsuche** eingegebenen Begriffe enthalten.

Wenn Sie die Filterung aufheben und alle Listeneinträge anzeigen möchten, klicken Sie auf **Löschen**.

Beispiel: Suchen von Erkennungsabfragen

Hier ist ein Beispiel für eine gültige Suche nach einer spezifischen Liste von Abfragen.

1 Klicken Sie auf **Menü** | **Abfragen und Berichte**. Klicken Sie auf **Abfrage**.

Alle in McAfee ePO verfügbaren Abfragen werden in der Liste angezeigt.

2 Beschränken Sie die Liste auf bestimmte Abfragen, zum Beispiel "Erkennung". Geben Sie im Feld **Schnellsuche** `Erkennung` ein, und klicken Sie dann auf **Übernehmen**.

Die folgenden Abfragen werden in der Liste angezeigt:

- **Malware-Entdeckungsverlauf**
- **Heutige Erkennungen pro Produkt**

Einige Listen enthalten Elemente, die für Ihren Standort übersetzt wurden. Bedenken Sie bei der Kommunikation mit Benutzern aus anderen Ländern, dass Abfragenamen anders lauten könnten.

Aktivieren der Kontrollkästchen von Tabellenzeilen

Auf der Benutzeroberfläche von ePolicy Orchestrator können Sie mithilfe spezieller Methoden und Tastenkombinationen die Tabellenzeilen auswählen. Dabei aktivieren Sie die Kontrollkästchen der einzelnen Tabellenzeilen, indem Sie entweder einfach **klicken** oder mit gedrückter **Umschalttaste** auf das Kontrollkästchen **klicken**.

Auf einigen Ausgabeseiten der ePolicy Orchestrator-Benutzeroberfläche wird neben jedem Listenelement einer Tabelle ein Kontrollkästchen angezeigt. Mithilfe dieser Kontrollkästchen können Sie einzelne, mehrere oder alle Zeilen in der Tabelle auswählen.

In der folgenden Tabelle sind die Tastenkombinationen aufgeführt, mit denen Sie die Kontrollkästchen von Tabellenzeilen aktivieren können.

Auswahl	Aktion	Ergebnis
Einzelne Zeilen	Klicken auf die Kontrollkästchen einzelner Zeilen	Die einzelnen Zeilen werden unabhängig voneinander ausgewählt.
Gruppe von Zeilen	Klicken Sie auf das Kontrollkästchen der ersten gewünschten Zeile, und **klicken** Sie dann mit gedrückter **Umschalttaste** auf das letzte gewünschte Kontrollkästchen.	Es wird eine Gruppe von Zeilen ausgewählt, die von der ersten bis zur letzten ausgewählten Zeile reicht. Wenn Sie durch **Klicken** bei gedrückter **Umschalttaste** mehr als 1.500 Zeilen gleichzeitig auswählen, kann dies zu einer zu hohen CPU-Auslastung führen und eine Fehlermeldung bezüglich eines Skriptfehlers auslösen.
Alle Zeilen	Klicken Sie auf das Kontrollkästchen ganz oben in der Tabellenüberschrift.	Es werden sämtliche Zeilen in der Tabelle ausgewählt.

Einrichten von ePolicy Orchestrator

Das Einrichten des ePolicy Orchestrator-Servers ist der erste Schritt zum Verwalten Ihrer Netzwerksicherheit.

Kapitel 3 *Planen der ePolicy Orchestrator-Konfiguration*
Kapitel 4 *Einrichten des McAfee ePO-Servers*
Kapitel 5 *Benutzerkonten und Berechtigungssätze*
Kapitel 6 *Repositories*
Kapitel 7 *Registrierte Server*
Kapitel 8 *Agentensteuerungen*

3 Planen der ePolicy Orchestrator-Konfiguration

Damit Sie den McAfee ePO-Server effizient nutzen können, müssen Sie einen umfassenden Plan für die jeweilige Umgebung erstellen.

Wie Sie Ihre Server-Infrastruktur einrichten und wie umfangreich die durchzuführenden Konfigurationsarbeiten sind, hängt von den jeweiligen Gegebenheiten Ihrer Netzwerkumgebung ab. Je sorgfältiger Sie diese Punkte im Voraus überdenken, desto schneller ist alles eingerichtet und funktionsbereit.

Inhalt

- *Erwägungen zur Skalierbarkeit*
- *Internetprotokolle in einer verwalteten Umgebung*

Erwägungen zur Skalierbarkeit

Wie Sie Ihre Skalierbarkeit verwalten, hängt davon ab, ob Sie mehrere McAfee ePO-Server, mehrere remote Agentensteuerungen oder beide verwenden.

Mit ePolicy Orchestrator können Sie Ihr Netzwerk vertikal oder horizontal skalieren.

- ***Vertikale Skalierbarkeit*** : Dies bedeutet, dass Sie größere, schnellere Hardware hinzufügen bzw. Upgrades auf solche Hardware durchführen können, um immer umfangreichere Bereitstellungen zu verwalten. Die vertikale Skalierung der McAfee ePO-Server-Infrastruktur wird durch ein Upgrade der Server-Hardware und Verwendung mehrerer McAfee ePO-Server im Netzwerk erreicht, die jeweils über eine eigene Datenbank verfügen.
- ***Horizontale Skalierbarkeit*** : Hierbei wird die Größe der Bereitstellung gesteigert, die von einem einzigen McAfee ePO-Server verwaltet werden kann. Erreicht wird dies durch Installation mehrerer Remote-Agenten-Handler, die sich jeweils bei einer einzigen Datenbank melden.

Verwenden mehrerer McAfee ePO-Server

Je nach Größe und Aufbau einer Organisation kann der Einsatz mehrerer McAfee ePO-Server erforderlich sein.

Der Einsatz mehrerer Server kann in Szenarien wie den folgenden erforderlich sein:

- Für jede Abteilung in Ihrem Unternehmen soll eine eigene Datenbank unterhalten werden.
- Es werden separate IT-Infrastrukturen, administrative Gruppen oder Testumgebungen benötigt.
- Das Unternehmen ist über mehrere geographische Standorte verteilt und nutzt eine Netzwerkverbindung mit relativ geringer Bandbreite, z. B. WAN, VPN oder andere langsamere Verbindungen, die meist zwischen remoten Standorten eingesetzt werden. Weitere Informationen zu Anforderungen bezüglich der Bandbreite finden Sie im *McAfee ePolicy Orchestrator-Handbuch zur Hardware-Dimensionierung und Bandbreitennutzung*.

Beim Einsatz mehrerer Server in einem Netzwerk ist es erforderlich, für jeden Server eine eigene Datenbank zu unterhalten. Die in den einzelnen Servern befindlichen Informationen können Sie auf dem McAfee ePO-Haupt-Server und der Hauptdatenbank zusammenfassen.

Verwenden mehrerer remoter Agentensteuerungen

Durch den Einsatz mehrerer remoter Agentensteuerungen können Sie größere Ausbringungen verwalten, ohne dass dafür zusätzliche McAfee ePO-Server zur Umgebung hinzugefügt werden müssen.

Die Agentensteuerung ist die Komponente des Servers, die für die Verwaltung von Agenten-Anforderungen zuständig ist. Jede McAfee ePO-Server-Installation verfügt standardmäßig über eine Agentensteuerung. Der Einsatz mehrerer remoter Agentensteuerungen kann in Szenarien wie den folgenden erforderlich sein:

- Sie möchten, dass Agenten zwischen mehreren physischen Geräten wählen können, damit sie auch im Falle eines nicht verfügbaren Anwendungsservers noch in der Lage sind, sich zu melden und Richtlinien-, Task- und Produktaktualisierungen abzurufen. Und Sie möchten dies erreichen, ohne dazu einen Cluster Ihres McAfee ePO-Servers zu erstellen.
- Die vorhandene ePolicy Orchestrator-Infrastruktur muss erweitert werden, um mehr Agenten, weitere Produkte oder eine aus kürzeren Agent-zu-Server-Kommunikationsintervallen resultierende höhere Arbeitslast zu bewältigen.
- Sie möchten mit Ihrem McAfee ePO-Server voneinander getrennte Netzwerksegmente verwalten, z. B. Systeme, die Network Address Translation (NAT) verwenden, oder sich in einem externen Netzwerk befinden.

> Dies funktioniert, solange die Agentensteuerung über eine Verbindung mit hoher Bandbreite zur ePolicy Orchestrator-Datenbank verfügt.

Durch den Einsatz mehrerer Agentensteuerungen kann die Skalierbarkeit erhöht und die Komplexität bei der Verwaltung umfangreicherer Ausbringungen verringert werden. Da Agentensteuerungen jedoch eine schnelle Netzwerkverbindung benötigen, gibt es Szenarien, für die sie eher nicht geeignet sind, wie zum Beispiel:

- Als Ersatz für verteilte Repositories. Verteilte Repositories sind lokale Dateifreigaben, mit denen der bei der Agenten-Kommunikation anfallende Datenverkehr niedrig gehalten werden soll. Auch wenn in Agentensteuerungen eine Repository-Funktion integriert ist, müssen Sie permanent mit der ePolicy Orchestrator-Datenbank kommunizieren und belegen daher einen deutlich größeren Anteil an Bandbreite.
- Zur Verbesserung der Repository-Replizierung über eine WAN-Verbindung. Der bei der Repository-Replizierung erforderliche permanente Kommunikationsfluss zur Datenbank kann die gesamte Bandbreite der WAN-Verbindung in Anspruch nehmen.
- Zum Verbinden eines abgetrennten Netzwerksegments, aus dem nur begrenzte oder unregelmäßige Verbindungen zur ePolicy Orchestrator-Datenbank erfolgen.

Internetprotokolle in einer verwalteten Umgebung

ePolicy Orchestrator ist mit beiden IP-Versionen kompatibel: IPv4 und IPv6.

McAfee ePO-Server arbeiten in drei verschiedenen Modi:

- **Nur IPv4**: Unterstützt nur das IPv4-Adressformat.
- **Nur IPv6**: Unterstützt nur das IPv6-Adressformat.
- **Gemischter Modus**: Unterstützt sowohl das IPv4- als auch das IPv6-Adressformat.

In welchem Modus ein McAfee ePO-Server arbeitet, hängt von der Netzwerkkonfiguration ab. Wenn das Netzwerk zum Beispiel so konfiguriert ist, dass nur IPv4-Adressen verwendet werden, arbeitet der Server im Modus "Nur IPv4". Wenn das Netzwerk dagegen so konfiguriert ist, dass sowohl IPv4- als auch IPv6-Adressen verwendet werden, arbeitet der Server im gemischten Modus.

Solange IPv6 nicht installiert und aktiviert ist, werden im McAfee ePO-Server nur Daten von IPv4-Adressen empfangen. Wenn IPv6 aktiviert ist, arbeitet der Server in dem Modus, in dem er konfiguriert ist.

Im Fall der Kommunikation per IPv6 des McAfee ePO-Servers mit einer Agentensteuerung werden adressrelevante Eigenschaften (beispielsweise IP-Adresse, Subnetzadresse und Subnetzmaske) im IPv6-Format gemeldet. Bei der Übertragung zwischen Client und McAfee ePO-Server oder bei der Anzeige in der Benutzeroberfläche oder Protokolldatei werden IPv6-relevante Eigenschaften in der erweiterten Form angezeigt und in Klammern gesetzt.

So wird zum Beispiel 3FFE:85B:1F1F::A9:1234 als [3FFE:085B:1F1F:0000:0000:0000:00A9:1234] angezeigt.

Beim Festlegen einer IPv6-Adresse für FTP- oder HTTP-Quellen sind keine Änderungen an der Adresse erforderlich. Beim Festlegen einer literalen IPv6-Adresse für eine UNC-Quelle müssen Sie jedoch das Microsoft-Format für literale IPv6-Adressen verwenden. Weitere Informationen dazu finden Sie in der Microsoft-Dokumentation.

4 Einrichten des McAfee ePO-Servers

Beschleunigen Sie die Einsatzbereitschaft der Software, indem Sie die grundlegenden Funktionen des McAfee ePO-Servers konfigurieren.

Inhalt

- *Überblick über die Server-Konfiguration*
- *Verwenden des Status der automatischen Produktinstallation*
- *Grundlegende Funktionen für die manuelle oder geführte Konfiguration*
- *Konfigurieren grundlegender Funktionen*
- *Verwenden eines Proxyservers*
- *Eingeben Ihres Lizenzschlüssels*
- *Konfigurieren von Product Improvement Program*
- *Deinstallieren von McAfee Product Improvement Program*

Überblick über die Server-Konfiguration

Es gibt mehrere Methoden, mit denen Sie den McAfee ePO-Server gemäß den individuellen Anforderungen der Umgebung einrichten können.

Sie müssen die folgenden grundlegenden Funktionen des McAfee ePO-Servers konfigurieren:

- **Status der Produktinstallation**: Startet automatisch die Installation und Konfiguration der lizenzierten Sicherheits-Software auf dem McAfee ePO-Server. Folgende Möglichkeiten stehen zur Verfügung:
  - Sie können zulassen, dass die standardmäßige Sicherheits-Software auf dem McAfee ePO-Server installiert wird.
  - Klicken Sie auf **Anhalten** und checken Sie mit dem **Software-Manager** von der Konsole aus manuell neue und aktualisierte Sicherheits-Software auf dem McAfee ePO-Server und im **Master-Repository** ein.

  Die Seite Status der Produktinstallation wird nur angezeigt, wenn Sie bei der Installation von McAfee ePO die Option **Automatische Produktinstallation aktivieren** ausgewählt haben.

- **Systemstruktur**: Enthält sämtliche über den McAfee ePO-Server verwaltete Systeme und ermöglicht das Durchführen von Aktionen auf diesen Systemen.
- **Richtlinienkatalog**: Hier konfigurieren Sie Sicherheitsrichtlinien, mit denen die auf den verwalteten Systemen ausgebrachte Sicherheitssoftware gesteuert wird.
- **Client-Task-Katalog** – Hier können Sie Client-Tasks erstellen, zuweisen und festlegen, dass Sie automatisch auf Ihren verwalteten Systemen ausgeführt werden.

Diese Tabelle enthält die Konfigurationsschritte für die automatische oder manuelle Installation der lizenzierten Produkt-Software.

Tabelle 4-1 Übersicht über die verschiedenen Konfigurationsmethoden

Automatischer Download der Produkt-Software	Manueller Download der Produkt-Software
1 Die ePolicy Orchestrator-Installation ist abgeschlossen, und Sie starten die Software. 2 Melden Sie sich auf dem Anmeldebildschirm bei der ePolicy Orchestrator-Benutzeroberfläche an. Die Seite Status der Produktinstallation wird angezeigt, und die neuesten Versionen der lizenzierten Sicherheits-Software werden auf dem McAfee ePO-Server installiert. Auf der Seite werden die Produkte und deren Status angezeigt. 3 Wenn der Status aller Produkte Abgeschlossen lautet, fahren Sie fort mit Schritt 5. Wenn für Produkte der Status Fehlgeschlagen angezeigt wird, aktivieren Sie das Kontrollkästchen neben dem Produktnamen, und klicken Sie auf **Wiederholen**. 4 Wenn bei der fehlgeschlagenen Produktinstallation weiterhin Fehler auftreten, gehen Sie wie folgt vor: • Laden Sie die Produkt-Software manuell herunter, um das fehlgeschlagene Produkt mit dem Software-Manager zu installieren. • Wenden Sie sich an den technischen Support von McAfee. • Fahren Sie mit der Konfiguration von McAfee ePO fort, und versuchen Sie später, die Produkt-Software zu installieren. 5 Führen Sie nach Bedarf die folgenden Schritte für die Umgebung aus: • Fügen Sie Systeme zur Systemstruktur hinzu. • Konfigurieren der allgemeinen Server-Einstellungen • Erstellen von Benutzerkonten • Konfigurieren von Berechtigungssätzen • Konfigurieren Sie Richtlinien. • Konfigurieren von erweiterten Server-Einstellungen und -Funktionen • Einrichten zusätzlicher Komponenten	1 Die ePolicy Orchestrator-Installation ist abgeschlossen, und Sie starten die Software. 2 Melden Sie sich auf dem Anmeldebildschirm bei der ePolicy Orchestrator-Benutzeroberfläche an. 3 Führen Sie die **geführte ePolicy Orchestrator-Konfiguration** für diese Vorgänge aus: • Hinzufügen von McAfee-Sicherheitssoftware zum Master-Repository • Hinzufügen von Systemen zur Systemstruktur • Erstellen und Zuweisen mindestens einer Sicherheitsrichtlinie auf den verwalteten Systemen • Planen eines Client-Aktualisierungs-Tasks • Bereitstellen der Sicherheitsprodukte auf den verwalteten Systemen Sie müssen die geführte Konfiguration nicht verwenden. Sie können jeden dieser Schritte auch manuell ausführen. 4 Führen Sie nach Bedarf die folgenden Schritte für die Umgebung aus: • Konfigurieren der allgemeinen Server-Einstellungen • Erstellen von Benutzerkonten • Konfigurieren von Berechtigungssätzen • Konfigurieren Sie Richtlinien. • Konfigurieren von erweiterten Server-Einstellungen und -Funktionen • Einrichten zusätzlicher Komponenten

Verwenden des Status der automatischen Produktinstallation

Die Seite Status der Produktinstallation wird automatisch angezeigt, wenn Sie sich erstmals bei McAfee ePO anmelden. Die Sicherheits-Software wird automatisch auf dem McAfee ePO-Server installiert. Sie können die Installation auch **anhalten** und die Sicherheits-Software manuell einchecken.

Bevor Sie beginnen

Die Seite Status der Produktinstallation wird nur angezeigt, wenn Sie bei der Installation von McAfee ePO die Option **Automatische Produktinstallation aktivieren** ausgewählt haben.

Die Seite Status der Produktinstallation ist nur in den ersten 24 Stunden nach der ersten Anmeldung bei McAfee ePO verfügbar. Bei allen späteren Benutzeranmeldungen wird die Seite mit dem Standard-Dashboard angezeigt. Nach 24 Stunden wird die Option Status der Produktinstallation aus der Liste unter **Menü** | **Automatisierung** entfernt.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf dem Desktop des ePolicy Orchestrator-Servers auf das Symbol **ePolicy Orchestrator starten**, damit der Bildschirm Anmelden angezeigt wird.

2 Geben Sie im Dialogfeld **Anmelden** die Anmeldeinformationen ein, und wählen Sie eine Sprache aus.

Die Seite Status der Produktinstallation wird angezeigt, und die für das Unternehmen verfügbare lizenzierte Software wird automatisch heruntergeladen und installiert. Mit den folgenden Optionen können Sie die automatische Software-Installation überwachen:

- **Produkte**: Zeigt alle lizenzierten Software-Produkte und die jeweils neueste verfügbare Version an.
- **Status**: Zeigt einen der folgenden Werte an:
  - **Aktualisierung**: Wird angezeigt, während die Software heruntergeladen und installiert wird.
  - **Abgeschlossen**: Wird angezeigt, wenn die Software erfolgreich installiert wurde.
  - **Fehlgeschlagen**: Wird angezeigt, wenn beim Download oder der Installation ein Fehler aufgetreten ist.
  - **Angehalten**: Wird angezeigt, wenn Sie oben auf der Seite auf **Anhalten** geklickt haben.

Sie können jederzeit auf **Menü** | **Software** | **Software-Manager** klicken, um Details zur Software-Installation anzuzeigen.

Außerdem können Sie auf der Benutzeroberfläche von McAfee ePO andere Elemente konfigurieren, während die Software-Installation ausgeführt wird.

3 Sie können die Software-Installation mit einer der in dieser Tabelle aufgeführten Methoden abschließen.

Automatische Installation	Manuelle Installation
Warten Sie, bis sich auf der Seite Status der Produktinstallation der **Status** der einzelnen Produkte in **Abgeschlossen** ändert. Wenn eine Produktinstallation fehlschlägt, aktivieren Sie das Kontrollkästchen neben dem Produktnamen, um die Installation erneut zu versuchen. Wenn die Installation weiterhin fehlschlägt, versuchen Sie, die Installation mit dem Software-Manager durchzuführen.	Klicken Sie auf der Seite Status der Produktinstallation auf **Anhalten**. Klicken Sie dann in dem Dialogfeld, in dem Ihnen mitgeteilt wird, dass Sie die Software-Installation mit dem **Software-Manager** durchführen müssen, auf OK. Die Werte für die Produktstatus ändern sich in Angehalten.
	Zum Durchführen der Software-Installation klicken Sie auf **Menü** | **Software** | **Software-Manager**. Detaillierte Anweisungen zum manuellen Durchführen der Software-Installation finden Sie unter *Software-Manager*.

4 Schließen Sie die ePolicy Orchestrator-Konfiguration ab, indem Sie nach Bedarf die folgenden Tasks ausführen:

- **Allgemeine Server-Einstellungen konfigurieren**: Server-Einstellungen aus dieser Gruppe betreffen Funktionen, die Sie für den ordnungsgemäßen Betrieb des Servers nicht ändern müssen, mit denen Sie jedoch einige Verhaltensweisen des Servers anpassen können.
- **Benutzerkonten erstellen und Berechtigungssätze konfigurieren**: Über Benutzerkonten können Benutzer auf den Server zugreifen. Über Berechtigungssätze werden Rechte und der Zugriff auf die Funktionen von ePolicy Orchestrator gewährt.
- **Erweiterte Server-Einstellungen und Funktionen konfigurieren**: Der McAfee ePO-Server verfügt über erweiterte Funktionen und Merkmale, mit denen Sie die Verwaltung der Netzwerksicherheit automatisieren können.
- **Zusätzliche Komponenten einrichten**: Zusätzliche Komponenten wie beispielsweise verteilte Repositories, registrierte Server und Agenten-Handler sind erforderlich, um viele der erweiterten Funktionen der ePolicy Orchestrator-Software zu verwenden.

Die verwalteten Systeme werden jetzt vom McAfee ePO-Server geschützt.

Grundlegende Funktionen für die manuelle oder geführte Konfiguration

Verschiedene Funktionen des McAfee ePO-Servers sind unerlässlich für die Verwendung und müssen bei der manuellen oder geführten Konfiguration eingerichtet werden. Diese Funktionen sind für die Bereitstellung und Verwaltung von Sicherheits-Software auf den Systemen im Netzwerk erforderlich.

Im Lieferumfang der McAfee ePO-Software ist das Tool Geführte Konfiguration enthalten. Mithilfe dieses Tools können Sie die grundlegenden Funktionen leichter konfigurieren und sich mit der Benutzeroberfläche von McAfee ePO vertraut machen. Die geführte Konfiguration hilft beim Durchführen der erforderlichen Schritte für die folgenden Aufgaben:

1 Einchecken von McAfee-Sicherheits-Software in das Master-Repository, damit die Software auf den Systemen im Netzwerk bereitgestellt werden kann Installieren der Produkt-Software auf der Seite Status der Produktinstallation oder mit dem Software-Manager

2 Hinzufügen der Systeme zur McAfee ePO-Systemstruktur, damit Sie sie verwalten können

3 Erstellen und Zuweisen mindestens einer Sicherheitsrichtlinie, die auf den verwalteten Systemen erzwungen werden soll

4 Planen eines Tasks für die Client-Aktualisierung, der die Sicherheitssoftware auf aktuellem Stand hält

5 Ausbringen der Sicherheits-Software auf den verwalteten Systemen

Sie müssen die geführte Konfiguration nicht verwenden. Wenn Sie die Schritte manuell ausführen, sollten Sie jedoch bei der Konfiguration einen ähnlichen Workflow einhalten. Unabhängig davon, nach welcher Vorgehensweise Sie diese Funktionen konfigurieren, können Sie die McAfee ePO-Konfiguration mithilfe des Tools Geführte Konfiguration oder direkt auf den einzelnen Seiten im Menü ändern.

Konfigurieren grundlegender Funktionen

Mit dem Tool Geführte Konfiguration können Sie grundlegende Funktionen konfigurieren. Sie können diese Tasks auch als Hilfestellung beim manuellen Konfigurieren eines McAfee ePO-Servers verwenden.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf dem Desktop des McAfee ePO-Servers auf das Symbol **ePolicy Orchestrator**, damit der Bildschirm Anmelden angezeigt wird.

2 Geben Sie den Benutzernamen und das Kennwort ein, wählen Sie gegebenenfalls eine Sprache aus, und klicken Sie auf **Anmelden**. ePolicy Orchestrator wird gestartet, und das Dialogfeld Dashboard wird angezeigt.

3 Installieren Sie die Produkt-Software über den Status der automatischen Produktinstallation oder über den Software-Manager. Details hierzu finden Sie unter *Verwenden des Status der automatischen Produktinstallation* oder unter *Software-Manager*.

4 Klicken Sie auf **Menü** | **Berichterstellung** | **Dashboards**, wählen Sie in der Dropdown-Liste **Dashboard** die Option **Geführte Konfiguration** aus, und klicken Sie dann auf **Starten**.

5 Lesen Sie die Übersicht und die Anweisungen zur Option **Geführte Konfiguration**, und klicken Sie dann auf **Starten**.

6 Gehen Sie auf der Seite **Software-Auswahl** wie folgt vor:

   a Klicken Sie unter der Produktkategorie **Nicht eingecheckte Software** auf **Lizenziert** oder **Test**, um die verfügbaren Produkte anzuzeigen.

   b Wählen Sie in der Tabelle **Software** das Produkt aus, das Sie einchecken möchten. Die Produktbeschreibung und alle verfügbaren Komponenten werden unten in der Tabelle angezeigt.

   c Klicken Sie auf **Alle einchecken**, um Produkterweiterungen in den McAfee ePO-Server und Produktpakete in das Master-Repository einzuchecken.

   d Klicken Sie oben im Bildschirm auf **Weiter**, wenn die Software eingecheckt ist und Sie mit dem nächsten Schritt fortfahren möchten.

7 Gehen Sie auf der Seite Systemauswahl wie folgt vor:

   a Wählen Sie aus, welcher Gruppe in der **Systemstruktur** die Systeme hinzugefügt werden sollen. Wenn noch keine benutzerdefinierten Gruppen vorhanden sind, wählen Sie **Eigene Organisation** aus, und klicken Sie dann auf **Weiter**. Das Dialogfeld Hinzufügen der Systeme wird geöffnet.

   b Wählen Sie aus, auf welche Weise Sie die Systeme der **Systemstruktur** hinzufügen möchten:

Methode	Aktion	Vorgehensweise
AD-Synchronisierung	Synchronisieren Sie den McAfee ePO-Server mit dem Active Directory-Server oder Domänen-Controller. Wenn in der Umgebung einer dieser Server vorhanden ist, stellt die AD-Synchronisierung die schnellste Möglichkeit dar, Systeme der **Systemstruktur** hinzuzufügen.	1 Wählen Sie im Dialogfeld AD-Synchronisierung den gewünschten Synchronisierungstyp aus, und geben Sie die entsprechenden Einstellungen an. 2 Klicken Sie auf **Synchronisieren** und **Speichern**, um mit dem nächsten Schritt fortzufahren.
Manuell	Sie können Systeme manuell der **Systemstruktur** hinzufügen, indem Sie ihre Namen angeben oder eine Liste mit Systemen pro Domäne durchsuchen.	1 Klicken Sie auf der Seite Neue Systeme auf **Durchsuchen**, um einzelne Systeme aus einer Domäne hinzuzufügen, und klicken Sie auf **OK**, oder geben Sie im Feld **Zielsysteme** Namen von Systemen ein. 2 Klicken Sie auf **Systeme hinzufügen**, um mit dem nächsten Schritt fortzufahren.

8 Gehen Sie auf der Seite **Richtlinienkonfiguration** wie folgt vor:

Option	Aktion	Vorgehensweise
Standardeinstellungen verwenden	Verwenden Sie für die Software, die Sie bereitstellen möchten, die Richtlinieneinstellung **My Default**, und setzen Sie die Konfiguration fort.	Damit ist dieser Schritt abgeschlossen.
Richtlinie konfigurieren	Geben Sie nun für die einzelnen Software-Produkte, die Sie eingecheckt haben, benutzerdefinierte Richtlinieneinstellungen an.	1 Klicken Sie im Dialogfeld Richtlinienkonfiguration auf **OK**. 2 Wählen Sie in der **Produktliste** ein Produkt aus, und klicken Sie auf **My Default**, um die Einstellungen der Default-Richtlinie zu bearbeiten. 3 Klicken Sie auf **Weiter**, um mit dem nächsten Schritt fortzufahren.

9 Gehen Sie auf der Seite **Software-Aktualisierung** wie folgt vor:

Option	Aktion	Vorgehensweise
Standardzeitplan erstellen	Erstellen Sie automatisch einen standardmäßigen Client-Produktaktualisierungs-Task, der täglich um 12:00 Uhr ausgeführt wird.	Damit ist dieser Schritt abgeschlossen.
Task-Plan festlegen	Konfigurieren Sie den Zeitplan für Ihren Client-Produktaktualisierungs-Task manuell.	1 Geben Sie im **Generator für Client-Task-Zuweisungen** ein **Produkt** und einen **Task-Namen** für Ihren Produktaktualisierungs-Task an. Ändern Sie nicht die Auswahl im Feld **Task-Typ**. Als **Task-Typ** muss **Produktaktualisierung** eingestellt sein. 2 Konfigurieren Sie die Optionen **Task-Vererbung sperren** und **Tags**, und klicken Sie dann auf **Weiter**. 3 Geben Sie den Zeitplan für den Aktualisierungs-Task an, und klicken Sie dann auf **Weiter**. 4 Überprüfen Sie die Zusammenfassung, und klicken Sie dann auf **Speichern**.

10 Gehen Sie auf der Seite Software-Bereitstellung wie folgt vor:

a Wählen Sie in der Systemstruktur den Speicherort der Systeme aus, auf denen Sie die Software ausbringen möchten. Klicken Sie dann auf **Weiter**. Klicken Sie auf **OK**, um fortzufahren.

b Geben Sie die Einstellungen für die McAfee Agent-Ausbringung an, und klicken Sie dann auf **Ausbringen**.

Wenn Sie diese Aktion zu einem späteren Zeitpunkt durchführen möchten, klicken Sie auf **Agenten-Ausbringung überspringen**. Sie können andere Sicherheits-Software jedoch erst dann ausbringen, wenn Agenten ausgebracht wurden.

c Wählen Sie die Software-Pakete aus, die Sie auf den verwalteten Systemen ausbringen möchten, und klicken Sie dann auf **Ausbringen**.

11 Klicken Sie auf der Seite **Konfigurationszusammenfassung** auf **Fertig stellen**, um die **geführte Konfiguration** zu schließen.

12 Schließen Sie die ePolicy Orchestrator-Konfiguration ab, indem Sie nach Bedarf die folgenden Tasks ausführen:

- **Konfigurieren der allgemeinen Server-Einstellungen**: Die Server-Einstellungen in dieser Gruppe betreffen Funktionen, die Sie für den ordnungsgemäßen Betrieb des Servers nicht ändern müssen. Wenn Sie möchten, können Sie jedoch einige Verhaltensweisen des Servers anpassen.
- **Benutzerkonten erstellen und Berechtigungssätze konfigurieren**: Über Benutzerkonten können Benutzer auf den Server zugreifen. Über Berechtigungssätze werden Rechte und der Zugriff auf die Funktionen von ePolicy Orchestrator gewährt.

- **Erweiterte Server-Einstellungen und Funktionen konfigurieren**: Der McAfee ePO-Server verfügt über erweiterte Funktionen und Merkmale, mit denen Sie die Verwaltung der Netzwerksicherheit automatisieren können.
- **Einrichten zusätzlicher Komponenten**: Für die Verwendung vieler erweiterter Funktionen von ePolicy Orchestrator sind zusätzliche Komponenten wie verteilte Repositories, registrierte Server und Agenten-Handler erforderlich.

Die verwalteten Systeme werden jetzt vom McAfee ePO-Server geschützt.

Verwenden eines Proxyservers

Wenn in der Netzwerkumgebung ein Proxyserver verwendet wird, müssen Sie die Proxyeinstellungen auf der Seite Server-Einstellungen angeben.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste **Einstellungskategorien** den Eintrag **Proxyeinstellungen** aus, und klicken Sie dann auf **Bearbeiten**.

2 Wählen Sie **Proxyeinstellungen manuell konfigurieren** aus, geben Sie die entsprechenden Konfigurationsinformationen an, die der Proxyserver für die einzelnen Gruppen von Optionen verwendet, und klicken Sie dann auf **Speichern**.

Eingeben Ihres Lizenzschlüssels

Ihr Lizenzschlüssel berechtigt Sie zu einer vollständigen Installation der Software und trägt die lizenzierten ePolicy Orchestrator-Produkte, die Ihr Unternehmen besitzt, in den McAfee-Software-Manager ein.

Ohne Lizenzschlüssel wird die Software im Testmodus ausgeführt. Nach Ablauf des Testzeitraums funktioniert die Software nicht mehr. Einen Lizenzschlüssel können Sie zu jedem beliebigen Zeitpunkt während oder nach Ablauf des Testzeitraums hinzufügen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste **Einstellungskategorien** den Eintrag **Lizenzschlüssel** aus, und klicken Sie dann auf **Bearbeiten**.

2 Geben Sie Ihren **Lizenzschlüssel** ein, und klicken Sie auf **Speichern**.

Konfigurieren von Product Improvement Program

Mit McAfee Product Improvement Program können McAfee-Produkte weiter verbessert werden. Mit diesem Programm werden proaktiv und in regelmäßigen Abständen Daten auf den vom McAfee ePO-Server verwalteten Client-Systemen erfasst.

Mit McAfee Product Improvement Program werden Daten zu den folgenden Aspekten erfasst:

- Systemumgebung (Software- und Hardware-Details)
- Effektivität von installierten McAfee-Produktfunktionen
- McAfee-Produktfehler und zugehörige Windows-Ereignisse

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste **Einstellungskategorien** den Eintrag **Product Improvement Program** aus, und klicken Sie dann auf **Bearbeiten**.
2. Wählen Sie **Ja** aus, um das Erfassen anonymer Diagnose- und Nutzungsdaten durch McAfee zuzulassen, und klicken Sie dann auf **Speichern**.

Klicken Sie hier, wenn Sie mehr über McAfee Product Improvement Program erfahren möchten.

Deinstallieren von McAfee Product Improvement Program

Das McAfee Product Improvement Program kann jederzeit deinstalliert werden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Melden Sie sich beim McAfee ePO-Server als Administrator an.
2. Klicken Sie auf **Menü** | **Richtlinie** | **Client-Task-Katalog**, wählen Sie bei **Client-Task-Typen** | **den Eintrag** McAfee Agent**Produktausbringung** aus, und klicken Sie dann auf **Aktionen** | **Neuer Task**.
3. Erstellen Sie einen neuen Task, um McAfee Product Improvement Program auf den gewünschten Client-Systemen zu deinstallieren.
4. Weisen Sie den Task den Client-Systemen zu, und senden Sie eine Agenten-Reaktivierung.
5. Klicken Sie auf **Menü** | **Software** | **Master-Repository**. Klicken Sie dann neben dem Paket **McAfee Product Improvement Program** auf **Löschen**. Klicken Sie anschließend auf **OK**.
6. Klicken Sie auf **Menü** | **Software** | **Erweiterungen**, und wählen Sie dann **McAfeeMcAfee Product Improvement Program** aus.
7. Klicken Sie auf **Entfernen** und dann auf **OK**.

5 Benutzerkonten und Berechtigungssätze

Jedem Benutzerkonto sind ein oder mehrere Berechtigungssätze zugewiesen, die festlegen, welche Aktionen der Benutzer mit der Software durchführen darf.

Inhalt

- *Benutzerkonten*
- *Client-Zertifikatauthentifizierung*
- *Berechtigungssätze*

Benutzerkonten

Mithilfe von Benutzerkonten können Sie steuern, auf welche Inhalte Benutzer zugreifen und wie sie die Software nutzen dürfen. Selbst in der kleinsten Netzwerkinstallation muss der Zugriff festgelegt und kontrolliert werden, den Benutzer auf die verschiedenen Teile des Systems haben.

Benutzerkonten können auf verschiedene Weisen erstellt und verwaltet werden. Folgende Möglichkeiten stehen zur Verfügung:

- Sie können Benutzerkonten manuell erstellen und dann jedem Konto einen geeigneten Berechtigungssatz zuweisen.
- Sie können den McAfee ePO-Server so konfigurieren, dass sich Benutzer über die Windows-Authentifizierung anmelden können.

Das Zulassen von Benutzeranmeldungen mithilfe von Windows-Anmeldeinformationen ist eine erweiterte Funktion, für die mehrere Einstellungen und Komponenten konfiguriert bzw. eingerichtet werden müssen.

Auch wenn Benutzerkonten und Berechtigungssätze in einer engen Beziehung zueinander stehen, werden sie auf unterschiedliche Weise erstellt und konfiguriert.

Inhalt

- *Verwalten von Benutzerkonten*
- *Unterstützte Formate für Benutzernamen und Kennwörter*
- *Erstellen einer benutzerdefinierten Anmeldenachricht*
- *Konfigurieren einer Active Directory-Benutzeranmeldung*
- *Das Audit-Protokoll*

Verwalten von Benutzerkonten

Auf der Seite **Benutzerverwaltung** können Sie Benutzerkonten manuell erstellen, bearbeiten und löschen.

Anstatt ein Konto zu löschen, sollten Sie dessen **Anmeldestatus** deaktivieren, bis Sie sicher sind, dass alle mit dem Konto verbundenen wichtigen Informationen zu anderen Benutzern verschoben wurden.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Öffnen Sie die Seite **Benutzerverwaltung**: Klicken Sie auf **Menü** | **Benutzerverwaltung** | **Benutzer**.

2 Wählen Sie eine der folgenden Aktionen aus.

Aktion	Vorgehensweise
Erstellen eines Benutzers	1 Klicken Sie auf **Neuer Benutzer**. 2 Geben Sie einen Benutzernamen ein. 3 Legen Sie fest, ob der Anmeldestatus dieses Kontos aktiviert oder deaktiviert werden soll. Wenn das Konto für eine Person gedacht ist, die noch nicht zu Ihrem Unternehmen gehört, möchten Sie es vielleicht erst einmal deaktivieren. 4 Wählen Sie aus, ob das neue Konto **McAfee ePO-Authentifizierung**, **Windows-Authentifizierung** oder **Zertifikatbasierte Authentifizierung** verwendet, und geben Sie die erforderlichen Anmeldeinformationen an, oder wechseln Sie zu dem Zertifikat, und wählen Sie es aus. 5 Optional können Sie im Textfeld **Anmerkungen** den vollständigen Namen, die E-Mail-Adresse, die Telefonnummer und eine Beschreibung des Benutzers eingeben. 6 Legen Sie fest, ob der Benutzer ein Administrator sein soll, oder wählen Sie für den Benutzer die entsprechenden Berechtigungssätze aus. 7 Klicken Sie auf **Speichern**, um zur Registerkarte Benutzer zurückzukehren. Der neue Benutzer wird auf der Seite **Benutzerverwaltung** in der Liste Benutzer angezeigt.
Bearbeiten eines Benutzers	1 Wählen Sie in der Liste **Benutzer** den zu bearbeitenden Benutzer aus, und klicken Sie dann auf **Aktion**	**Bearbeiten**. 2 Nehmen Sie die gewünschten Änderungen am Konto vor. 3 Klicken Sie auf **Speichern**. Die geänderten Benutzerdaten werden auf der Seite **Benutzerverwaltung** in der Liste Benutzer angezeigt.
Löschen eines Benutzers	1 Wählen Sie in der Liste **Benutzer** den zu löschenden Benutzer aus, und klicken Sie dann auf **Aktion**	**Löschen**. 2 Wenn Sie dazu aufgefordert werden, klicken Sie auf **OK**. Der Benutzer wird nicht mehr auf der Seite **Benutzerverwaltung** in der Liste Benutzer angezeigt.

Siehe auch

Unterstützte Formate für Benutzernamen und Kennwörter auf Seite 42

Unterstützte Formate für Benutzernamen und Kennwörter

Überprüfen Sie diese unterstützten Formate beim Erstellen von Benutzernamen und Kennwörtern für SQL-Datenbanken.

Alle druckbaren Zeichen aus dem Zeichensatz ISO8859-1 werden unterstützt. Dabei gelten die folgenden Ausnahmen.

Plattform	Nicht unterstützte Zeichen für Kennwörter und Benutzernamen
McAfee ePO	• Voran- oder nachgestellte Leerzeichen oder Kennwörter, die nur aus Leerzeichen bestehen • Doppelte Anführungszeichen (") • Vorangestellte umgekehrte Schrägstriche (\) • Doppelpunkte in Benutzernamen (:) • Semikolons in Benutzernamen (;)

Siehe auch

Verwalten von Benutzerkonten auf Seite 41

Erstellen einer benutzerdefinierten Anmeldenachricht

Sie können eine benutzerdefinierte Anmeldenachricht erstellen und anzeigen, die auf der Seite **Anmelden** erscheinen soll.

Die Nachricht kann als einfacher Text oder im HTML-Format geschrieben sein. Wenn Sie eine Nachricht im HTML-Format erstellen, sind Sie für alle Formatierungen und das Escaping verantwortlich.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste **Einstellungskategorien** den Eintrag **Anmeldenachricht** aus, und klicken Sie dann auf **Bearbeiten**.
2. Wählen Sie **Benutzerdefinierte Anmeldenachricht anzeigen** aus, geben Sie die gewünschte Nachricht ein, und klicken Sie anschließend auf **Speichern**.

Konfigurieren einer Active Directory-Benutzeranmeldung

Durch die Konfiguration einer Active Directory-Benutzeranmeldung können Sie den Arbeitsaufwand senken, der mit der Verwaltung der Benutzerkonten sowie des Benutzerzugriffs verbunden ist.

Inhalt

- *Verwalten von ePolicy Orchestrator-Benutzern mit Active Directory*
- *Strategien für die Windows-Authentifizierung und -Autorisierung*
- *Aktivieren der Windows-Authentifizierung im McAfee ePO-Server*
- *Konfigurieren der Windows-Authentifizierung*
- *Konfigurieren der Windows-Autorisierung*

Verwalten von ePolicy Orchestrator-Benutzern mit Active Directory

Sie können vorhandene Windows-authentifizierte Benutzeranmeldeinformationen verwenden, um automatisch ePolicy Orchestrator-Benutzer zu erstellen und diesen Berechtigungen zuzuweisen.

Dies wird erreicht, indem ePolicy Orchestrator-Berechtigungssätze zu Active Directory-Gruppen in Ihrer Umgebung zugeordnet werden. Bei einer großen Anzahl von ePolicy Orchestrator-Benutzern in einem Unternehmen kann mit dieser Funktion der Verwaltungsaufwand verringert werden. Gehen Sie folgendermaßen vor, um die Konfiguration vorzunehmen:

- Konfigurieren Sie die Benutzerauthentifizierung.
- Registrieren Sie die LDAP-Server.
- Weisen Sie der Active Directory-Gruppe Berechtigungssätze zu.

Benutzerauthentifizierung

ePolicy Orchestrator-Benutzer können mittels ePolicy Orchestrator-Kennwortauthentifizierung oder Windows-Authentifizierung authentifiziert werden. Bei Verwendung der Windows-Authentifizierung können Sie angeben, nach welchen Merkmalen Benutzer authentifiziert werden:

- Anhand der Domäne, zu der Ihr McAfee ePO-Server gehört (Standardeinstellung)
- Anhand einer Liste mit einem oder mehreren Domänen-Controllern
- Anhand einer Liste mit einem oder mehreren Domänennamen im DNS-Format
- Mithilfe eines WINS-Servers zum Auffinden des entsprechenden Domänen-Controllers

Wenn Sie Domänen-Controller, DNS-Domänennamen oder einen WINS-Server verwenden, müssen Sie die Server-Einstellung **Windows-Authentifizierung** konfigurieren.

Registrierte LDAP-Server

Sie müssen LDAP-Server bei Ihrem McAfee ePO-Server registrieren, um dynamisch zugewiesene Berechtigungssätze für Windows-Benutzer zuzulassen. Dynamisch zugewiesene Berechtigungssätze sind Berechtigungssätze, die Benutzern anhand deren Mitgliedschaft in Active Directory-Gruppen zugeordnet werden.

Benutzer, denen über unidirektionale externe Vertrauensstellungen vertraut wird, werden nicht unterstützt.

Das Benutzerkonto, mit dem der LDAP-Server bei ePolicy Orchestrator registriert ist, muss über eine bidirektionale transitive Vertrauensstellung als vertrauenswürdig gelten, oder es muss in der Domäne physisch vorhanden sein, zu der der LDAP-Server gehört.

Windows-Autorisierung

Die Server-Einstellung für die Windows-Autorisierung gibt an, welchen Active Directory-Server ePolicy Orchestrator verwendet, um Benutzer- und Gruppeninformationen für eine bestimmte Domäne zu sammeln. Sie können mehrere Domänen-Controller und Active Directory-Server angeben. Mit dieser Server-Einstellung können Sie Benutzern, die beim Anmelden Windows-Anmeldeinformationen angeben, Berechtigungssätze dynamisch zuweisen.

ePolicy Orchestrator kann Windows-authentifizierten Benutzern selbst bei deaktivierter Active Directory-Benutzeranmeldung Berechtigungssätze dynamisch zuweisen.

Zuweisen von Berechtigungen

Sie müssen mindestens einen Berechtigungssatz zu einer Active Directory-Gruppe zuweisen, bei der es sich nicht um die primäre Gruppe eines Benutzers handelt. Das dynamische Zuweisen von Berechtigungssätzen zur primären Gruppe eines Benutzers wird nicht unterstützt und führt dazu, dass nur die Berechtigungen gelten, die diesem Benutzer manuell zugewiesen wurden. In der Standardeinstellung ist "Domänen-Benutzer" die primäre Gruppe.

Active Directory-Benutzeranmeldung

Wenn Sie die oben aufgeführten Punkte konfiguriert haben, können Sie die Server-Einstellung zur automatischen Benutzererstellung aktivieren. Mithilfe automatischer Benutzererstellung können Benutzerdatensätze unter den folgenden Bedingungen automatisch erstellt werden:

- Benutzer geben gültige Anmeldeinformationen im Format <Domäne\Name> an. So würde zum Beispiel ein Benutzer mit dem Windows-Anmeldenamen "mmustermann1", der Mitglied in der Windows-Domäne "deu" ist, die folgenden Anmeldeinformationen angeben: "deu\mmustermann1" und das entsprechende Kennwort.
- Ein Active Directory-Server, der Informationen zu diesem Benutzer enthält, wurde bei ePolicy Orchestrator registriert.
- Der Benutzer ist Mitglied in mindestens einer Gruppe vom Typ "Lokal (in Domäne)" oder "Global (in Domäne)", die einem ePolicy Orchestrator-Berechtigungssatz zugeordnet ist.

Strategien für die Windows-Authentifizierung und -Autorisierung

Es gibt verschiedene Ansätze, nach denen Sie beim Planen der Registrierung Ihrer LDAP-Server vorgehen können. Wenn Sie sich im Vorfeld ausreichend Zeit für die Planung einer Strategie für die Server-Registrierung nehmen, werden Sie gleich beim ersten Mal alles richtig machen und haben auch weniger Probleme bei der Benutzerauthentifizierung.

Im Idealfall müssen Sie diesen Vorgang nur einmal durchführen und Änderungen nur dann vornehmen, wenn sich Ihre Netzwerktopologie insgesamt ändert. Sobald die Server registriert sind und die Windows-Authentifizierung konfiguriert ist, sollten Sie diese Einstellungen nicht mehr allzu oft ändern müssen.

Vergleich von Authentifizierung und Autorisierung

Bei der Authentifizierung wird die Identität eines Benutzers verifiziert. Dabei werden die vom Benutzer angegebenen Anmeldeinformationen mit Informationen verglichen, denen das System als authentisch vertraut. Das können ein McAfee ePO-Server-Konto, Active Directory-Anmeldeinformationen oder ein Zertifikat sein. Wenn Sie die Windows-Authentifizierung verwenden möchten, müssen Sie untersuchen, auf welche Weise die Domänen (oder Server) organisiert sind, in denen sich Ihre Benutzerkonten befinden.

Die Autorisierung erfolgt, nachdem die Anmeldeinformationen eines Benutzers überprüft wurden. Hierbei werden Berechtigungssätze angewendet, die bestimmen, was der Benutzer innerhalb des Systems durchführen darf. Bei Verwendung der Windows-Authentifizierung können Sie festlegen, welche Aktionen Benutzern aus unterschiedlichen Domänen erlaubt sein sollen. Dies erfolgt über Berechtigungssätze, die Gruppen in diesen Domänen zugewiesen werden.

Netzwerktopologie für Benutzerkonten

Welche Schritte zur vollständigen Konfiguration der Windows-Authentifizierung und -Autorisierung erforderlich sind, richtet sich nach der Netzwerktopologie und der Verteilung der Benutzerkonten im Netzwerk.

- Wenn sich die Anmeldeinformationen für Ihre zukünftigen Benutzer alle in einer kleinen Auswahl von Domänen (oder Server) innerhalb einer einzigen Domänenstruktur befinden, müssen Sie nur den Stamm dieser Struktur registrieren – mehr nicht.
- Wenn Ihre Benutzerkonten breiter verteilt sind, müssen Sie eine größere Anzahl von Servern oder Domänen registrieren. Ermitteln Sie, wie viele Domänen-Unterstrukturen (oder Server-Unterstrukturen) Sie mindestens benötigen, und registrieren Sie die Stämme dieser Strukturen. Versuchen Sie, diese in der Reihenfolge zu registrieren, in der sie am häufigsten verwendet werden. Da die Liste der Domänen (oder Server) beim Authentifizierungsvorgang in der aufgeführten Reihenfolge durchlaufen wird, wirkt es sich positiv auf die durchschnittliche Authentifizierungsleistung aus, wenn sich die am häufigsten verwendeten Domänen oder Server oben in der Liste befinden.

Berechtigungsstruktur

Damit ein Benutzer sich mittels Windows-Authentifizierung bei einem McAfee ePO-Server anmelden kann, muss mit der in seiner Domäne befindlichen Active Directory-Gruppe, zu der sein Konto gehört, ein Berechtigungssatz verbunden sein. Bei der Frage, wie Berechtigungssätze zugewiesen sein sollen, müssen Sie folgende Punkte beachten:

- Berechtigungssätze können mehreren Active Directory-Gruppen zugewiesen werden.
- Berechtigungssätze können dynamisch nur einer gesamten Active Directory-Gruppe zugewiesen werden. Sie können nicht nur einigen Benutzern aus einer Gruppe zugewiesen werden.

Wenn Sie einem einzelnen Benutzer spezielle Berechtigungen zuweisen möchten, können Sie dies durchführen, indem Sie eine Active Directory-Gruppe erstellen, in der sich nur dieser jeweilige Benutzer befindet.

Aktivieren der Windows-Authentifizierung im McAfee ePO-Server

Bevor die erweiterte Windows-Authentifizierung verwendet werden kann, muss der Server entsprechend vorbereitet werden.

Zum Aktivieren der Seite Windows-Authentifizierung in den Server-Einstellungen müssen Sie zuerst den ePolicy Orchestrator-Dienst beenden. Dieser Schritt muss direkt auf dem McAfee ePO-Server ausgeführt werden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie in der Server-Konsole auf **Start** | **Einstellungen** | **Systemsteuerung** | **Verwaltung**.
2. Wählen Sie **Dienste** aus.
3. Klicken Sie im Fenster **Dienste** mit der rechten Maustaste auf **McAfee ePolicy Orchestrator-Anwendungs-Server**, und wählen Sie **Beenden** aus.
4. Benennen Sie die Datei `WINAUTH.DLL` in `WINAUTH.BAK` um.

   In einer Standardinstallation befindet sich diese Datei in `C:\Programme\McAfee\ePolicy Orchestrator\Server\bin`.
5. Starten Sie den Server neu.

Wenn Sie die Seite Server-Einstellungen das nächste Mal öffnen, wird die Option **Windows-Authentifizierung** angezeigt.

Konfigurieren der Windows-Authentifizierung

Es gibt mehrere Möglichkeiten, wie vorhandene Anmeldeinformationen für Windows-Konten in ePolicy Orchestrator verwendet werden können.

> **Bevor Sie beginnen**
>
> Sie müssen Ihren Server zunächst für die Windows-Authentifizierung vorbereitet haben.

Wie Sie diese Einstellungen konfigurieren, hängt von verschiedenen Aspekten ab:

- Möchten Sie mehrere Domänen-Controller verwenden?
- Sind die Benutzer über mehrere Domänen verteilt?
- Möchten Sie mithilfe eines WINS-Servers suchen, anhand welcher Domäne Benutzer authentifiziert werden sollen?

Ohne besondere Konfiguration können sich Benutzer mit Windows-Anmeldeinformationen für die Domäne authentifizieren, zu der der McAfee ePO-Server gehört, oder mit Anmeldeinformationen jeder anderen Domäne, die in einer wechselseitigen Vertrauensstellung zur Domäne des McAfee ePO-Servers steht. Wenn Benutzer aus Domänen vorhanden sind, die diese Kriterien nicht erfüllen, müssen Sie die Windows-Authentifizierung konfigurieren.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, und klicken Sie dann in der Liste **Einstellungskategorien** auf **Windows-Authentifizierung**.
2. Klicken Sie auf **Bearbeiten**.
3. Geben Sie an, ob Sie eine oder mehrere Domänen, einen oder mehrere Domänen-Controller oder einen WINS-Server verwenden möchten.

   Domänen müssen im DNS-Format angegeben werden (z. B. `interneDomäne.com`). Domänen-Controller und WINS-Server müssen vollqualifizierte Domänennamen haben (z. B. `dc .interneDomäne.com`).

   Sie können mehrere Domänen oder Domänen-Controller, aber nur einen WINS-Server angeben. Klicken Sie auf **+**, um weitere Domänen oder Domänen-Controller zur Liste hinzuzufügen.
4. Wenn Sie alle gewünschten Server hinzugefügt haben, klicken Sie auf **Speichern**.

Wenn Sie Domänen oder Domänen-Controller angeben, geht der McAfee ePO-Server beim Authentifizieren von Benutzern die Server in der aufgeführten Reihenfolge durch. Zuerst wird die Authentifizierung beim ersten in der Liste eingetragenen Server versucht, und dann wird die Liste abwärts abgearbeitet, bis ein Benutzer erfolgreich authentifiziert ist.

Konfigurieren der Windows-Autorisierung

Damit Benutzer sich erfolgreich mit Windows-Authentifizierung bei einem McAfee ePO-Server anmelden können, benötigen sie einen Berechtigungssatz, der einer ihrer Active Directory-Gruppen zugewiesen ist.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Benutzerverwaltung** | **Berechtigungssätze**.
2. Wählen Sie entweder in der Liste **Berechtigungssätze** einen vorhandenen Berechtigungssatz aus, und klicken Sie dann im Abschnitt **Name und Benutzer** auf **Bearbeiten**, oder klicken Sie auf **Neuer Berechtigungssatz**.
3. Wählen Sie einzelne Benutzer aus, für die der Berechtigungssatz gilt.
4. Wählen Sie in der Liste einen **Server-Namen** aus, und klicken Sie auf **Hinzufügen**.

5 Wechseln Sie im LDAP-Browser zu den Gruppen, für die dieser Berechtigungssatz gilt, und wählen Sie sie aus.

Wenn Sie im Bereich **Durchsuchen** ein Element auswählen, werden im Bereich **Gruppen** die Mitglieder dieses Elements angezeigt. Sie können eine beliebige Anzahl dieser Gruppen auswählen, die den Berechtigungssatz dynamisch erhalten sollen. Es können immer nur Mitglieder aus einem Element gleichzeitig hinzugefügt werden. Zum Hinzufügen von Mitgliedern aus mehreren Elementen müssen Sie die Schritte 4 und 5 so oft wiederholen, bis alle gewünschten Mitglieder hinzugefügt sind.

6 Klicken Sie auf **Speichern**.

Der Berechtigungssatz wird auf alle Benutzer aus den angegebenen Gruppen angewendet, die sich mit Windows-Authentifizierung beim Server anmelden.

Das Audit-Protokoll

Verwenden Sie das Audit-Protokoll, um eine Aufzeichnung aller ePolicy Orchestrator-Benutzeraktionen aufzurufen und zu verwalten. Die Einträge im Audit-Protokoll werden in einer sortierbaren Tabelle angezeigt. Zwecks größerer Flexibilität können Sie das Protokoll auch so filtern, dass nur fehlgeschlagene Aktionen oder nur Einträge eines bestimmten Alters angezeigt werden.

Das Audit-Protokoll besteht aus sieben Spalten:

- **Aktion**: Der Name der Aktion, die der ePolicy Orchestrator-Benutzer auszuführen versuchte.
- **Endzeit** – Der Zeitpunkt, zu dem die Aktion abgeschlossen wurde.
- **Details** – Weitere Informationen zur Aktion.
- **Priorität** – Die Bedeutung der Aktion.
- **Startzeit** – Der Zeitpunkt, zu dem die Aktion gestartet wurde.
- **Erfolgreich** – Gibt an, ob die Aktion erfolgreich abgeschlossen wurde.
- **Benutzername** – Der Benutzername des angemeldeten Benutzerkontos, mit dem die Aktion ausgeführt wurde.

Audit-Protokollinformationen werden in der Sprache angezeigt, die als Gebietsschema des Unternehmensadministrators eingestellt ist.

Die Einträge im Audit-Protokoll können abgefragt werden. Sie können mit dem Assistenten Abfrage-Generator Abfragen für diese Daten erstellen oder die Standardabfragen für diese Daten verwenden. Mit der Abfrage Fehlgeschlagene Anmeldeversuche wird beispielsweise eine Tabelle aller fehlgeschlagenen Anmeldeversuche abgerufen.

Siehe auch

Anzeigen und Bereinigen des Audit-Protokolls auf Seite 48
Planmäßiges Bereinigen des Audit-Protokolls auf Seite 49

Anzeigen und Bereinigen des Audit-Protokolls

Sie können den Verlauf von Benutzeraktionen anzeigen und bereinigen.

Welche Daten beim Anzeigen des Audit-Protokolls verfügbar sind, hängt davon ab, wie oft und bei welchem Alter das Audit-Protokoll bereinigt wird.

Beim Bereinigen des Audit-Protokolls werden die Datensätze dauerhaft gelöscht.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Benutzerverwaltung** | **Audit-Protokoll**. Das Audit-Protokoll wird angezeigt.

2 Wählen Sie eine der folgenden Aktionen aus.

Aktion	Vorgehensweise
Anzeigen des Audit-Protokolls	1 Klicken Sie auf einen Spaltentitel, um die Tabelle nach der betreffenden Spalte (alphabetisch) zu sortieren. 2 Wählen Sie in der Dropdown-Liste **Filter** eine Option aus, um die angezeigte Datenmenge einzugrenzen. Sie können alle Aktionen bis auf die fehlgeschlagenen entfernen oder nur die Aktionen anzeigen, die in einem ausgewählten Zeitrahmen erfolgten. 3 Klicken Sie auf einen Eintrag, um dessen Details anzuzeigen.
Bereinigen des Audit-Protokolls	1 Klicken Sie auf **Aktionen**	**Bereinigen**. 2 Geben Sie im Dialogfeld Bereinigen neben **Datensätze bereinigen, die älter sind als** eine Zahl ein, und wählen Sie eine Zeiteinheit aus. 3 Klicken Sie auf **OK**. Alle Datensätze im Audit-Protokoll werden dauerhaft gelöscht.

Siehe auch

Das Audit-Protokoll auf Seite 48

Planmäßiges Bereinigen des Audit-Protokolls

Mit einem geplanten Server-Task können Sie das Audit-Protokoll automatisch bereinigen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Öffnen Sie den **Generator für Server-Tasks**.

   a Wählen Sie die folgenden Optionen aus: **Menü** | **Automatisierung** | **Server-Tasks**.

   b Klicken Sie auf **Neuer Task**.

2 Geben Sie einen Namen und eine Beschreibung für den Task ein. Wählen Sie neben Planungsstatus die Option **Aktiviert** aus, und klicken Sie dann auf **Weiter**.

3 Wählen Sie in der Dropdown-Liste die Option **Audit-Protokoll bereinigen** aus.

4 Geben Sie hinter **Datensätze bereinigen, die älter sind als:** einen Zeitraum (Dauer und Einheit) an, nachdem die Einträge im Audit-Protokoll bereinigt werden.

5 Klicken Sie auf **Weiter**.

6 Planen Sie den Task nach Bedarf, und klicken Sie dann auf **Weiter**.

7 Überprüfen Sie die Task-Details, und klicken Sie dann auf **Speichern**.

Siehe auch

Das Audit-Protokoll auf Seite 48

Client-Zertifikatauthentifizierung

Clients können ein digitales Zertifikat als Anmeldeinformationen für die Authentifizierung verwenden, wenn sie sich bei einem McAfee ePO-Server anmelden.

Inhalt

- *Verwenden der Client-Zertifikatauthentifizierung*
- *Konfigurieren von ePolicy Orchestrator für die Client-Zertifikatauthentifizierung*
- *Ändern der zertifikatbasierten Authentifizierung von McAfee ePO-Server*
- *Deaktivieren der Client-Zertifikatauthentifizierung von McAfee ePO-Server*
- *Konfigurieren von Benutzern für zertifikatbasierte Authentifizierung*
- *Aktualisieren der CRL-Datei*
- *Probleme bei der Client-Zertifikatauthentifizierung*
- *SSL-Zertifikate*
- *Erstellen eines selbstsignierten Zertifikats mit OpenSSL*
- *Weitere nützliche OpenSSL-Befehle*
- *Konvertieren einer vorhandenen PVK-Datei in eine PEM-Datei*

Verwenden der Client-Zertifikatauthentifizierung

Die Client-Zertifikatauthentifizierung ist die sicherste der zur Verfügung stehenden Methoden. Sie ist jedoch nicht in jeder Umgebung auch die beste Wahl.

Die Client-Zertifikatauthentifizierung ist eine Erweiterung der Authentifizierung mit öffentlichem Schlüssel. Als Grundlage dienen öffentliche Schlüssel, aber anders als bei der Authentifizierung mit öffentlichem Schlüssel muss nur einem vertrauenswürdigen Drittanbieter vertraut werden, der als *Zertifizierungsstelle* bekannt ist. Zertifikate sind digitale Dokumente, die eine Kombination von Identitätsinformationen und öffentlichen Schlüsseln enthalten und von der Zertifizierungsstelle, die die Richtigkeit der Informationen überprüft, digital signiert werden.

Vorteile zertifikatbasierter Authentifizierung

Die zertifikatbasierte Authentifizierung weist gegenüber der Authentifizierung mittels Kennwort mehrere Vorteile auf:

- Zertifikate haben eine vorab festgelegte Gültigkeitsdauer. Dadurch wird eine erzwungene, periodische Überprüfung der Berechtigungen eines Benutzers bei Ablauf des Zertifikats ermöglicht.
- Wenn der Zugriff eines Benutzers gesperrt oder beendet werden muss, kann das Zertifikat zu einer *Zertifikatsperrliste* hinzugefügt werden, die bei jedem Anmeldeversuch geprüft wird, um unbefugten Zugriff zu vermeiden.
- Da nur einer geringen Anzahl von Zertifizierungsstellen – meist nur einer – vertraut werden muss, ist die zertifikatbasierte Authentifizierung in großen Institutionen leichter zu verwalten und besser skalierbar als andere Formen der Authentifizierung.

Nachteile zertifikatbasierter Authentifizierung

Nicht jede Umgebung ist für eine zertifikatbasierte Authentifizierung geeignet. Zu den Nachteilen dieser Methode gehören:

- Es ist eine Infrastruktur mit öffentlichem Schlüssel erforderlich. Dadurch können zusätzliche Kosten entstehen, die in einigen Fällen das Mehr an Sicherheit nicht wert sind.
- Im Vergleich zur Authentifizierung mittels Kennwort bringt diese Methode einen zusätzlichen Arbeitsaufwand beim Verwalten von Zertifikaten mit sich.

Konfigurieren von ePolicy Orchestrator für die Client-Zertifikatauthentifizierung

Damit sich Benutzer mithilfe der zertifikatbasierten Authentifizierung anmelden können, muss ePolicy Orchestrator entsprechend konfiguriert werden.

> **Bevor Sie beginnen**
> Sie müssen ein signiertes Zertifikat im Format P7B, PKCS12, DER oder PEM besitzen.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**.
2. Wählen Sie **Zertifikatbasierte Authentifizierung** aus, und klicken Sie auf **Bearbeiten**.
3. Wählen Sie **Zertifikatbasierte Authentifizierung aktivieren** aus.
4. Klicken Sie neben **Client-Zertifikat der Zertifizierungsstelle** auf die Schaltfläche **Durchsuchen**.
5. Wechseln Sie zu der Zertifikatdatei, wählen Sie sie aus, und klicken Sie auf **OK**.
6. Wenn Sie über eine **Datei mit Zertifikatsperrliste** (CRL-Datei) verfügen, klicken Sie neben diesem Bearbeitungsfeld auf die Schaltfläche **Durchsuchen**, wechseln Sie zu der CRL-Datei, und klicken Sie auf **OK**.
7. Klicken Sie auf **Speichern**, um alle Änderungen zu speichern.
8. Starten Sie ePolicy Orchestrator neu, um die zertifikatbasierte Authentifizierung zu aktivieren.

Ändern der zertifikatbasierten Authentifizierung von McAfee ePO-Server

Server benötigen Zertifikate für SSL-Verbindungen, die höhere Sicherheit als Standard-HTTP-Sitzungen bieten.

> **Bevor Sie beginnen**
> Um ein signiertes Zertifikat hochladen zu können, müssen Sie bereits ein Server-Zertifikat von einer Zertifizierungsstelle erhalten haben.

Sie können auch selbstsignierte Zertifikate anstelle von extern signierten Zertifikaten verwenden, dies birgt jedoch ein etwas höheres Risiko. Mit der nachfolgend beschriebenen Vorgehensweise kann eine zertifikatbasierte Authentifizierung erstmalig konfiguriert oder eine vorhandene Konfiguration mit einem aktualisierten Zertifikat geändert werden.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**.
2. Wählen Sie **Zertifikatbasierte Authentifizierung** aus, und klicken Sie auf **Bearbeiten**.
3. Wählen Sie **Zertifikatbasierte Authentifizierung aktivieren** aus.
4. Klicken Sie neben **Client-Zertifikat der Zertifizierungsstelle** auf die Schaltfläche **Durchsuchen**. Wechseln Sie zu der Zertifikatdatei, wählen Sie sie aus, und klicken Sie auf **OK**.

   Sobald eine Datei übernommen wurde, ändert sich die Eingabeaufforderung zu **Aktuelles Zertifizierungsstellen-Zertifikat ersetzen**.

5. Wenn Sie eine PKCS12-Zertifikatdatei angegeben haben, geben Sie ein Kennwort ein.

6 Wenn Sie eine Datei mit Zertifikatsperrliste (CRL) bereitstellen möchten, klicken Sie neben **Datei mit Zertifikatsperrliste (PEM)** auf **Durchsuchen**. Wechseln Sie zur Zertifikatsperrlisten-Datei, wählen Sie sie aus, und klicken Sie auf **OK**.

Die Zertifikatsperrlisten-Datei muss im PEM-Format vorliegen.

7 Falls erforderlich, wählen Sie erweiterte Einstellungen aus.

8 Klicken Sie auf **Speichern**, um alle Änderungen zu speichern.

9 Starten Sie den Server neu, um die Änderungen an den Einstellungen von für die zertifikatbasierte Authentifizierung zu aktivieren.

Deaktivieren der Client-Zertifikatauthentifizierung von McAfee ePO-Server

Server-Zertifikate können und sollten deaktiviert werden, wenn sie nicht mehr verwendet werden.

Bevor Sie beginnen

Bevor Sie Server-Zertifikate deaktivieren können, muss der Server bereits für die Client-Zertifikatauthentifizierung konfiguriert sein.

Nachdem ein Server-Zertifikat geladen wurde, kann es nur noch deaktiviert, aber nicht mehr entfernt werden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Öffnen Sie die Seite **Server-Einstellungen**, indem Sie **Menü** | **Konfiguration** | **Server-Einstellungen** auswählen.

2 Wählen Sie **Zertifikatbasierte Authentifizierung** aus, und klicken Sie auf **Bearbeiten**.

3 Deaktivieren Sie **Zertifikatbasierte Authentifizierung aktivieren**, und klicken Sie dann auf **Speichern**.

Die Server-Einstellungen wurden geändert. Sie müssen den Server jedoch neu starten, um den Vorgang abzuschließen.

Konfigurieren von Benutzern für zertifikatbasierte Authentifizierung

Damit Benutzer sich mit ihren digitalen Zertifikaten anmelden können, muss die zertifikatbasierte Authentifizierung konfiguriert sein.

Die für die zertifikatbasierte Authentifizierung verwendeten Zertifikate befinden sich meist auf einer Smartcard oder einem ähnlichen Gerät. Die Zertifikatdatei kann mithilfe einer Software aus dem Lieferumfang der Smartcard-Hardware extrahiert werden. Diese extrahierte Zertifikatdatei ist normalerweise die Datei, die in dem hier beschriebenen Verfahren hochgeladen wird.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Benutzerverwaltung** | **Benutzer**.

2 Wählen Sie einen Benutzer aus, und klicken Sie auf **Aktionen** | **Bearbeiten**.

3 Wählen Sie **Authentifizierung oder Anmeldeinformationen ändern** aus, und wählen Sie dann **Zertifikatbasierte Authentifizierung** aus.

4 Geben Sie die Anmeldeinformationen nach einer der hier beschriebenen Methoden an.

- Kopieren Sie das Feld für den eindeutigen Namen (DN-Feld) aus der Zertifikatdatei, und fügen Sie es in das Bearbeitungsfeld **Betrefffeld für eindeutigen Namen des persönlichen Zertifikats** ein.
- Laden Sie die Zertifikatdatei hoch, die mit dem Zertifizierungsstellen-Zertifikat signiert wurde, das Sie im Abschnitt *Konfigurieren von ePolicy Orchestrator für die zertifikatbasierte Authentifizierung* hochgeladen haben. Klicken Sie auf **Durchsuchen**, wechseln Sie zu der Zertifikatdatei auf Ihrem Computer, wählen Sie sie aus, und klicken Sie auf **OK**.

Benutzerzertifikate können PEM- oder DER-codiert sein. Solange das Format X.509- oder PKCS12-konform ist, spielt es jedoch keine Rolle, in welchem Format das Zertifikat vorliegt.

5 Klicken Sie auf **Speichern**, um die an der Konfiguration des Benutzers vorgenommenen Änderungen zu speichern.

Die angegebenen Zertifikatinformationen werden überprüft. Falls sie ungültig sind, wird eine Warnung ausgegeben. Wenn ein Benutzer versucht, sich bei ePolicy Orchestrator von einem Browser aus anzumelden, auf dem sein Zertifikat installiert ist, wird von nun an das Anmeldeformular ausgegraut angezeigt und der Benutzer sofort authentifiziert.

Aktualisieren der CRL-Datei

Sie können die auf dem McAfee ePO-Server installierte CRL-Datei (Zertifikatsperrliste) aktualisieren, um den Zugriff bestimmter Benutzer auf ePolicy Orchestrator zu unterbinden.

Bevor Sie beginnen

Es muss bereits eine CRL-Datei im ZIP- oder PEM-Format vorliegen.

Die CRL-Datei besteht aus einer Liste gesperrter ePolicy Orchestrator-Benutzer mit dem Status ihrer digitalen Zertifikate. Die Liste enthält die gesperrten Zertifikate, die Gründe für die Sperrung, den Zeitpunkt der Zertifikatsaustellung und die ausstellende Körperschaft. Wenn ein Benutzer versucht, auf den McAfee ePO-Server zuzugreifen, wird in der CRL-Datei geprüft, ob dem Benutzer der Zugriff gewährt werden darf oder nicht.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**.

2 Wählen Sie **Zertifikatbasierte Authentifizierung** aus, und klicken Sie auf **Bearbeiten**.

3 Klicken Sie zum Aktualisieren der **Datei mit Zertifikatsperrliste** (CRL-Datei) auf die Schaltfläche **Durchsuchen** neben diesem Bearbeitungsfeld, wechseln Sie zur CRL-Datei, und klicken Sie dann auf **OK**.

4 Klicken Sie auf **Speichern**, um alle Änderungen zu speichern.

5 Starten Sie ePolicy Orchestrator neu, um die zertifikatbasierte Authentifizierung zu aktivieren.

Sie können die CRL-Datei auch mithilfe der cURL-Befehlszeile aktualisieren. Geben Sie dazu in der cURL-Befehlszeile Folgendes ein:

Damit cURL-Befehle per Befehlszeile ausgeführt werden können, muss cURL installiert sein, und Sie müssen Remote-Zugriff auf den McAfee ePO-Server haben. Ausführliche Informationen zum Download von cURL und weitere Beispiele finden Sie im *Skripthandbuch zu ePolicy Orchestrator 5.0.0*.

```
curl -k --cert <Admin-Zertifikat>.pem --key <Admin-Schlüssel>.pem https://
<localhost>:<Port>/remote/console.cert.updatecrl.do -F crlFile=@<CRLs>.zip
```

Die einzelnen Parameter bedeuten Folgendes:

- `<Admin-Zertifikat>` – Der Name der PEM-Datei mit dem Administrator-Client-Zertifikat
- `<Admin-Schlüssel>` – Der Name der PEM-Datei mit dem privaten Administrator-Client-Schlüssel
- `<localhost>:<Port>` – Name und Nummer des Kommunikationsports des McAfee ePO-Servers
- `<CRLs>` – Der Name der CRL-PEM- oder -ZIP-Datei

Nun wird bei jedem Zugriff eines Benutzers auf den McAfee ePO-Server in der neuen CRL-Datei geprüft, ob die zertifikatbasierte Authentifizierung für diesen Benutzer widerrufen wurde.

Probleme bei der Client-Zertifikatauthentifizierung

Die meisten Probleme bei der zertifikatbasierten Authentifizierung werden von einer kleinen Anzahl von Problemen verursacht.

Wenn sich ein Benutzer mit seinem Zertifikat nicht bei ePolicy Orchestrator anmelden kann, sollten Sie eine der folgenden Möglichkeiten ausprobieren, um das Problem zu beheben:

- Stellen Sie sicher, dass der Benutzer nicht deaktiviert wurde.
- Überprüfen Sie, ob das Zertifikat abgelaufen ist oder zurückgenommen wurde.
- Überprüfen Sie, ob das Zertifikat von der richtigen Zertifizierungsstelle signiert wurde.
- Überprüfen Sie, ob das Feld für den eindeutigen Namen auf der Benutzerkonfigurationsseite korrekt ist.
- Vergewissern Sie sich, dass der Browser das richtige Zertifikat angibt.
- Überprüfen Sie das Audit-Protokoll auf Authentifizierungsmeldungen.

SSL-Zertifikate

In den von McAfee ePO unterstützten Browsern wird eine Warnung bezüglich eines SSL-Zertifikats des Servers angezeigt, wenn nicht überprüft werden kann, ob ein Zertifikat gültig ist oder von einer vertrauenswürdigen Quelle signiert wurde. Vom McAfee ePO-Server wird für die SSL-Kommunikation mit dem Web-Browser standardmäßig ein selbstsigniertes Zertifikat verwendet, das vom Browser in der Standardeinstellung nicht als vertrauenswürdig eingestuft wird. Daher wird jedes Mal, wenn Sie zur McAfee ePO-Konsole wechseln, eine Warnmeldung angezeigt.

Wenn diese Warnung nicht mehr angezeigt werden soll, müssen Sie einen der folgenden Schritte durchführen:

- Fügen Sie das McAfee ePO-Server-Zertifikat zur Sammlung der vom Browser verwendeten vertrauenswürdigen Zertifikate hinzu.

  Diesen Schritt müssen Sie für jeden einzelnen Browser vornehmen, über den Sie mit McAfee ePO interagieren. Wenn sich das Server-Zertifikat ändert, müssen Sie das McAfee ePO-Server-Zertifikat erneut hinzufügen, da das vom Server gesendete Server-Zertifikat nicht mehr mit dem Zertifikat übereinstimmt, für dessen Verwendung der Browser konfiguriert wurde.

- Ersetzen Sie das standardmäßige McAfee ePO-Server-Zertifikat durch ein gültiges Zertifikat, das von einer vom Browser als vertrauenswürdig eingestuften Zertifizierungsstelle signiert wurde. Das ist der beste Weg. Da das Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle signiert wurde, müssen Sie es nicht zu sämtlichen Web-Browsern im Unternehmen hinzufügen.

  Wenn sich der Server-Host-Name ändert, können Sie das Server-Zertifikat durch ein anderes Zertifikat ersetzen, das ebenfalls von einer vertrauenswürdigen Zertifizierungsstelle signiert wurde.

Um das McAfee ePO-Server-Zertifikat ersetzen zu können, müssen Sie sich zuerst ein neues Zertifikat besorgen – vorzugsweise ein Zertifikat, das von einer vertrauenswürdigen Zertifizierungsstelle signiert wurde. Außerdem benötigen Sie den privaten Schlüssel des Zertifikats und gegebenenfalls dessen Kennwort. Dann können Sie mit allen diesen Dateien das Zertifikat des Servers ersetzen. Weitere Informationen zum Ersetzen von Server-Zertifikaten finden Sie unter *Beschreibung und Funktionsweise von Sicherheitsschlüsseln*.

Vom McAfee ePO-Browser wird in den verknüpften Dateien das folgende Format erwartet:

- Server-Zertifikat – P7B oder PEM
- Privater Schlüssel – PEM

Wenn das Server-Zertifikat oder der private Schlüssel in einem anderen Format vorliegen, müssen sie in eines der unterstützten Formate konvertiert werden, bevor sie zum Ersetzen des Server-Zertifikats verwendet werden können.

Ersetzen des Server-Zertifikats

In den **Server-Einstellungen** können Sie das Server-Zertifikat und den privaten Schlüssel angeben, die von ePolicy Orchestrator verwendet werden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, und klicken Sie dann in der Liste **Einstellungskategorien** auf **Server-Zertifikat**.
2. Klicken Sie auf **Bearbeiten**. Die Seite **Server-Zertifikat: Bearbeiten** wird angezeigt.
3. Wechseln Sie zu der Datei mit dem Server-Zertifikat, und klicken Sie auf **Öffnen**.
4. Wechseln Sie zu der Datei mit dem privaten Schlüssel, und klicken Sie auf **Öffnen**.
5. Geben Sie bei Bedarf das Kennwort für den privaten Schlüssel ein.
6. Klicken Sie auf **Speichern**.

Nachdem Sie das neue Zertifikat und den neuen privaten Schlüssel übernommen haben, müssen Sie ePolicy Orchestrator neu starten, damit die Änderungen wirksam werden.

Installieren des Sicherheitszertifikats bei Verwendung von Internet Explorer

Verhindern Sie, dass die Zertifikataufforderung bei jeder Anmeldung angezeigt wird, indem Sie das Sicherheitszertifikat installieren.

Vorgehensweise

1. Starten Sie ePolicy Orchestrator in einem Browser. Die Seite Zertifikatfehler: Navigation wurde geblockt wird geöffnet.
2. Klicken Sie auf **Laden dieser Website fortsetzen (nicht empfohlen)**, um die Anmeldeseite zu öffnen. Die Adressleiste ist rot, wodurch angezeigt wird, dass der Browser das Sicherheitszertifikat nicht verifizieren kann.
3. Klicken Sie rechts neben der Adressleiste auf **Zertifikatfehler**, um die Warnung **Zertifikat ist ungültig** anzuzeigen.

4 Klicken Sie unten in der Warnung auf **Zertifikate anzeigen**, um das Dialogfeld **Zertifikat** zu öffnen.

Klicken Sie auf der Registerkarte **Allgemein** nicht auf **Zertifikat installieren**. Andernfalls schlägt der Vorgang fehl.

5 Klicken Sie auf die Registerkarte **Zertifizierungspfad**, wählen Sie dann **Orion_CA_<Servername>** aus, und klicken Sie auf **Zertifikat anzeigen**. Auf der Registerkarte **Allgemein** wird ein weiteres Dialogfeld geöffnet, in dem die Zertifikatinformationen angezeigt werden.

6 Klicken Sie auf **Zertifikat installieren**, um den **Zertifikatsimport-Assistenten** zu öffnen.

7 Klicken Sie auf **Weiter**, um anzugeben, wo sich das Zertifikat befindet.

8 Wählen Sie **Alle Zertifikate in folgendem Speicher speichern** aus, und klicken Sie dann auf **Durchsuchen**, um einen Speicherort auszuwählen.

9 Wählen Sie in der Liste den Ordner **Vertrauenswürdige Stammzertifizierungsstellen** aus, klicken Sie auf **OK**, und klicken Sie dann auf **Weiter**.

10 Klicken Sie auf **Fertig stellen**. Klicken Sie in der daraufhin angezeigten Sicherheitswarnung auf **Ja**.

11 Schließen Sie den Browser.

12 Ändern Sie das Ziel der Desktop-Verknüpfung für ePolicy Orchestrator so, dass der NetBIOS-Name des McAfee ePO-Servers verwendet wird (statt "localhost").

13 Starten Sie ePolicy Orchestrator neu.

Dann werden Sie beim Anmelden bei ePolicy Orchestrator nicht mehr aufgefordert, das Zertifikat zu akzeptieren.

Installieren des Sicherheitszertifikats bei Verwendung von Firefox 3.5 (oder höher)

Bei Verwendung von Firefox 3.5 (oder höher) können Sie das Sicherheitszertifikat installieren, damit nicht bei jeder Anmeldung das Dialogfeld mit dem Warnhinweis angezeigt wird.

Vorgehensweise

1 Starten Sie ePolicy Orchestrator vom Browser aus. Die Seite Sichere Verbindung fehlgeschlagen wird angezeigt.

2 Klicken Sie unten auf der Seite auf **Oder Sie können eine Ausnahme hinzufügen**. Nun wird auf der Seite die Schaltfläche Ausnahme hinzufügen angezeigt.

3 Klicken Sie auf **Ausnahme hinzufügen**. Das Dialogfeld Sicherheits-Ausnahmeregel hinzufügen wird angezeigt.

4 Klicken Sie auf **Zertifikat herunterladen**. Die Angaben zum Zertifizierungsstatus sind nun eingetragen, und die Schaltfläche Sicherheits-Ausnahmeregel bestätigen ist aktiviert.

5 Vergewissern Sie sich, dass **Diese Ausnahme dauerhaft speichern** aktiviert ist, und klicken Sie dann auf **Sicherheits-Ausnahmeregel bestätigen**.

Von nun an werden Sie beim Anmelden bei ePolicy Orchestrator nicht mehr aufgefordert, das Zertifikat zu akzeptieren.

Erstellen eines selbstsignierten Zertifikats mit OpenSSL

Manchmal können oder möchten Sie nicht warten, bis ein Zertifikat von einer Zertifizierungsstelle authentifiziert wurde. Bei ersten Tests oder bei Systemen, die in internen Netzwerken genutzt werden, kann ein selbstsigniertes Zertifikat ein ausreichendes Maß an Sicherheit und Funktionalität bieten.

Bevor Sie beginnen

Zum Erstellen eines selbstsignierten Zertifikats müssen Sie OpenSSL für Windows installieren. OpenSSL ist unter der folgenden URL-Adresse verfügbar:

http://www.slproweb.com/products/Win32OpenSSL.html

Verwenden Sie OpenSSL für Windows, wenn Sie ein Zertifikat für Ihren McAfee ePO-Server erstellen und selbst signieren möchten.

Es gibt viele Tools, mit denen selbstsignierte Zertifikate erstellt werden können. Hier wird die Vorgehensweise unter Verwendung von OpenSSL beschrieben.

Die im nachfolgenden Task verwendete Dateistruktur sieht wie folgt aus:

Diese Ordner werden nicht standardmäßig von OpenSSL nicht erstellt. Sie werden in diesen Beispielen verwendet und können erstellt werden, damit Sie Ihre Ausgabedateien leichter finden.

- **C:\ssl** – Der Installationsordner für OpenSSL.
- **C:\ssl\certs** – Hier werden die erstellten Zertifikate gespeichert.
- **C:\ssl\keys** – Hier werden die erstellten Schlüssel gespeichert.
- **C:\ssl\requests** – Hier werden die erstellten Zertifizierungsanforderungen gespeichert.

Vorgehensweise

1 Geben Sie den folgenden Befehl in einer Befehlszeile ein, um den anfänglichen Zertifikatschlüssel zu generieren:

```
C:\ssl\bin>openssl genrsa -des3 -out C:/ssl/keys/ca.key 1024
```

Der folgende Bildschirm wird angezeigt.

```
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.........................++++++
.++++++
unable to write 'random state'
e is 65537 (0x10001)
Enter pass phrase for keys/ca.key:
Verifying - Enter pass phrase for keys/ca.key:

C:\ssl\bin>
```

2 Geben Sie bei der ersten Eingabeaufforderung eine Passphrase ein, und geben Sie diese dann zur Bestätigung ein zweites Mal ein.

Notieren Sie sich die eingegebene Passphrase gut. Sie werden sie später noch benötigen.

Eine Datei mit dem Namen ca.key wird generiert und im Ordner `C:\ssl\keys\` gespeichert.

Der Schlüssel sieht in etwa so aus:

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,CE327E8D510D1882

4Evg9bqeteKbo6OWyOcFh6o8gUhcOTDn/odppSeykvQBAasEhFfcF+nHLort8KkS
bS9WDAqczf6SdKMxoGbi9m57X/PZ+7dcTH7YyKNKskfoqED7/VZXktAEhA1Vw+wj
.
.
.
im2DEkLWQ3kI+6HdaQHoOFe99ReHZJzvAU6F6LbUNULLpDe3wvnGwMI68lfAF9C3
4+KDIt1RhfK3piLpCOM+8L1Dpd0g5FC723Z1DrrOuwghKdyDlGRKLw==
-----END RSA PRIVATE KEY-----
```

3 Geben Sie den folgenden Befehl in einer Befehlszeile ein, um den erstellten Zertifikatschlüssel selbst zu signieren:

```
openssl req -new -x509 -days 365 -key C:/ssl/keys/ca.key -out C:/ssl/certs/ca.cer
```

Der folgende Bildschirm wird angezeigt.

```
Enter pass phrase for ca.key:
Loading 'screen' into random state - done
You are about to be asked to enter information that will be
incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished
Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Oregon
Locality Name (eg, city) []:Beaverton
Organization Name (eg, company) [Internet Widgits Pty Ltd]:McAfee
Organizational Unit Name (eg, section) []:Enterprise
Common Name (eg, YOUR name) []:ePO_Server
Email Address []:tester@mcafee.com

C:\ssl\bin>
```

Geben Sie nach den folgenden Eingabeaufforderungen die erforderlichen Informationen ein:

- Country Name (2 letter code) [AU]:
- State or Province Name (full name) [Some-State]:
- Locality Name (eg, city) []:
- Organization Name (eg, company) [Internet Widgits Pty Ltd]:

- Organizational Unit Name (eg, section) []:
- Common Name (eg, YOUR name) []:

  Geben Sie bei dieser Eingabeaufforderung den Namen Ihres Servers ein (z. B. den Namen des McAfee ePO-Servers).

- Email Address []:

Eine Datei mit dem Namen ca.cer wird generiert und im Ordner `C:\ssl\certs\` gespeichert.

Das selbstsignierte Zertifikat sieht in etwa wie folgt aus:

```
-----BEGIN CERTIFICATE-----
MIIDdTCCAt6gAwIBAgIJAJe1id+IhOGDMA0GCSqGSIb3DQEBBQUAMIGEMQswCQYD
VQQGEwJVUzEPMA0GA1UECBMGT1JFR090MRIwEAYDVQQHEwlCRUFWRVJUT04xDzAN
.
.
.
NF/Om6VMhuUy4Cyc5CIyTmGzVPDEo8dK2OkdLR+tQhDsdqM5qpfd6w52ew20RKo/
dLGiMtraicXeR2GyWrKJjywow3xBtkvyQQj2xmMWUmDwYjC0YH0lKjV0X+fGwcdX
jWTfB10HV8507ASU0qte0we/BSTMuZWgMA==
-----END CERTIFICATE-----
```

Wenn Sie ein signiertes Zertifikat für ePolicy Orchestrator von einem Drittanbieter (z. B. VeriSign oder der Microsoft Windows-Unternehmenszertifizierungsstelle) erstellen lassen möchten, finden Sie Informationen dazu im KnowledgeBase-Artikel KB72477.

4 Sie können das Zertifikat auf den McAfee ePO-Server hochladen und dort verwalten.

Weitere nützliche OpenSSL-Befehle

Sie können weitere OpenSSL-Befehle verwenden, um die in PKCS12-Zertifikaten generierten Schlüssel zu extrahieren sowie zu kombinieren, und um eine kennwortgeschützte private Schlüssel-PEM-Datei in eine nicht kennwortgeschützte Datei umzuwandeln.

Befehle für die Verwendung mit PKCS12-Zertifikaten

Mit den folgenden Befehlen können Sie ein PKCS12-Zertifikat erstellen, bei dem sich sowohl das Zertifikat als auch der Schlüssel in einer einzigen Datei befinden.

Beschreibung	OpenSSL-Befehlsformat
Erstellt ein Zertifikat und einen Schlüssel in der gleichen Datei.	`openssl req -x509 -nodes -days 365 -newkey rsa: 1024 -config` *Pfad* `\openssl.cnf -keyout` *Pfad* `\pkcs12Example.pem -out` *Pfad* `\pkcs12Example.pem`
Exportiert die PKCS12-Version des Zertifikats.	`openssl pkcs12 -export -out` *Pfad* `\pkcs12Example.pfx -in` *Pfad* `\pkcs12Example.pem -name "` *Benutzername* `"`

Mit den folgenden Befehlen können Sie das Zertifikat und den Schlüssel aus einem kombinierten PKCS12-Zertifikat trennen.

Beschreibung	OpenSSL-Befehlsformat
Extrahiert den PEM-Schlüssel aus der PFX-Datei.	`openssl pkcs12 -in pkcs12ExampleKey.pfx -out pkcs12ExampleKey.pem`
Entfernt das Kennwort im Schlüssel.	`openssl rsa -in pkcs12ExampleKey.pem -out pkcs12ExampleKeyNoPW.pem` Auf dem ePolicy Orchestrator-Server kann dann die Datei pkcs12ExampleCert.pem als Zertifikat und die Datei pkcs12ExampleKey.pem als Schlüssel (oder der Schlüssel ohne Kennwort pkcs12ExampleKeyNoPW.pem) verwendet werden.

Befehl zum Umwandeln einer kennwortgeschützten privaten Schlüssel-PEM-Datei

Geben Sie den folgenden Befehl ein, um eine kennwortgeschützte private Schlüssel-PEM-Datei in eine nicht kennwortgeschützte Datei umzuwandeln:

```
openssl rsa -in C:\ssl\keys\key.pem -out C:\ssl\keys\keyNoPassword.pem
```

Im vorherigen Beispiel steht "C:\ssl\keys" für den Eingabe- und den Ausgabepfad für die Dateien "key.pem" und "keyNoPassword.pem".

Konvertieren einer vorhandenen PVK-Datei in eine PEM-Datei

Der ePolicy Orchestrator-Browser unterstützt PEM-codierte private Schlüssel. Dazu gehören sowohl kennwortgeschützte als auch nicht durch Kennwörter geschützte private Schlüssel. Mithilfe von OpenSSL können Sie einen Schlüssel aus dem PVK- in das PEM-Format konvertieren.

Bevor Sie beginnen

Zum Konvertieren der PVK-Datei müssen Sie OpenSSL für Windows installieren. Diese Software ist unter der folgenden URL-Adresse verfügbar:

http://www.slproweb.com/products/Win32OpenSSL.html

Konvertieren Sie Ihr Zertifikat mithilfe von OpenSSL für Windows aus dem PVK- in das PEM-Format.

Vorgehensweise

1 Geben Sie den folgenden Befehl in der Befehlszeile ein, um eine zuvor erstellte PVK-Datei in eine PEM-Datei zu konvertieren:

```
openssl rsa -inform PVK -outform PEM -in C:\ssl\keys\myPrivateKey.pvk -out C:\ssl
\keys\myPrivateKey.pem -passin pass:p@$$w0rd -passout pass:p@$$w0rd
```

Die Argumente "-passin" und "-passout" im oben gezeigten Befehl sind optional.

2 Wenn Sie dazu aufgefordert werden, geben Sie das Kennwort ein, mit dem Sie die PKV-Datei erstellt haben.

Wenn das Argument "-passout" im oben gezeigten Beispiel nicht verwendet wird, ist der neu erstellte Schlüssel im PEM-Format nicht kennwortgeschützt.

Berechtigungssätze

Mit Berechtigungssätzen wird die Ebene des Zugriffs kontrolliert, den Benutzer auf in der Software verfügbare Funktionen haben.

Selbst in der kleinsten ePolicy Orchestrator-Installation muss der Zugriff festgelegt und kontrolliert werden, den Benutzer auf die verschiedenen Teile des Systems haben.

Inhalt

- *Das Zusammenspiel von Benutzern, Gruppen und Berechtigungssätzen*
- *Verwalten von Berechtigungssätzen*

Das Zusammenspiel von Benutzern, Gruppen und Berechtigungssätzen

Der Zugriff auf Elemente in ePolicy Orchestrator wird durch das Zusammenspiel von Benutzern, Gruppen und Berechtigungssätzen gesteuert.

Benutzer

Es gibt zwei allgemeine Kategorien von Benutzern: die Administratoren, die volle Rechte im System haben, und die normalen Benutzer. Normalen Benutzern kann eine beliebige Anzahl von Berechtigungssätzen zugewiesen werden, die deren Zugriffsebenen in ePolicy Orchestrator definieren.

Benutzerkonten können auf verschiedene Weisen erstellt und verwaltet werden. Folgende Möglichkeiten stehen zur Verfügung:

- Sie können Benutzerkonten manuell erstellen und dann jedem Konto einen geeigneten Berechtigungssatz zuweisen.
- Sie können den McAfee ePO-Server so konfigurieren, dass sich Benutzer mittels Windows-Authentifizierung anmelden können.

Das Zulassen von Benutzeranmeldungen mithilfe von Windows-Anmeldeinformationen ist eine erweiterte Funktion, für die mehrere Einstellungen und Komponenten konfiguriert bzw. eingerichtet werden müssen. Weitere Informationen zu dieser Möglichkeit finden Sie unter *Verwalten von ePolicy Orchestrator-Benutzern mit Active Directory*.

Auch wenn Benutzerkonten und Berechtigungssätze in einer engen Beziehung zueinander stehen, werden sie auf unterschiedliche Weise erstellt und konfiguriert. Weitere Informationen zu Berechtigungssätzen finden Sie unter *Verwalten von Berechtigungssätzen*.

Administratoren

Administratoren besitzen die Berechtigung zum Lesen und Schreiben sowie zum Ausführen aller Vorgänge. Beim Installieren des Servers wird automatisch ein Administratorkonto erstellt. In der Standardeinstellung lautet der Benutzername für dieses Konto **admin**. Wenn der Standardwert während der Installation geändert wird, wird dieses Konto entsprechend umbenannt.

Sie können für Benutzer, die Administratorrechte benötigen, weitere Administratorkonten erstellen.

Zu den Berechtigungen, die nur Administratoren vorbehalten sind, gehören die folgenden:

- Erstellen, Bearbeiten und Löschen von Quellsites und alternativen Sites
- Ändern von Server-Einstellungen
- Hinzufügen und Löschen von Benutzerkonten

- Hinzufügen, Löschen und Zuweisen von Berechtigungssätzen
- Importieren von Ereignissen in ePolicy Orchestrator-Datenbanken und Einschränken der Ereignisse, die dort gespeichert werden

Gruppen

Den Gruppen werden Abfragen und Berichte zugewiesen. Eine Gruppe kann privat (nur für den jeweiligen Benutzer), global öffentlich ("freigegeben") oder für ein oder mehrere Berechtigungssätze freigegeben sein.

Berechtigungssätze

In einem Berechtigungssatz wird ein bestimmtes Zugriffsprofil definiert. Das beinhaltet meist eine Kombination von Zugriffsebenen für verschiedene Teile von ePolicy Orchestrator. So kann zum Beispiel ein einzelner Berechtigungssatz die Erlaubnis zum Lesen des Audit-Protokolls, zum Verwenden öffentlicher und freigegebener Dashboards sowie zum Erstellen und Bearbeiten öffentlicher Berichte und Abfragen erteilen.

Berechtigungssätze können einzelnen Benutzern oder – bei Verwendung von Active Directory – allen Benutzern von bestimmten Active Directory-Servern zugewiesen werden.

Verwalten von Berechtigungssätzen

Auf der Seite Berechtigungssätze können Sie den Benutzerzugriff steuern und Berechtigungssätze erstellen, ändern, exportieren sowie importieren.

Die fertig definierten Berechtigungssätze können Sie am einfachsten migrieren, indem Sie sie exportieren und dann auf die anderen Server importieren.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Öffnen Sie die Seite **Berechtigungssätze**: Wählen Sie die folgenden Optionen aus: **Menü** | **Benutzerverwaltung** | **Berechtigungssätze**.

2 Wählen Sie eine der folgenden Aktionen aus:

Aktion	Vorgehensweise
Hinzufügen eines Berechtigungssatzes	**1** Klicken Sie auf **Neuer Berechtigungssatz**. **2** Geben Sie einen Namen für den neuen Berechtigungssatz ein. Die Verwendung eines bereits vorhandenen Namens ist nicht zulässig. Jeder Berechtigungssatz muss einen eindeutigen Namen besitzen. **3** Wenn Sie diesem Berechtigungssatz sofort bestimmte Benutzer zuweisen möchten, wählen Sie die Namen der gewünschten Benutzer im Abschnitt Benutzer aus. **4** Wenn Sie diesem Berechtigungssatz Active Directory-Gruppen zuordnen möchten, wählen Sie in der Liste **Server-Name** den Server aus, und klicken Sie dann auf **Hinzufügen**. **5** Wenn Sie hinzugefügte Active Directory-Server entfernen möchten, wählen Sie die gewünschten Server im Listenfeld Active Directory aus, und klicken Sie dann auf **Entfernen**. **6** Klicken Sie zum Speichern des Berechtigungssatzes auf **Speichern**. Der Berechtigungssatz ist erstellt, ihm sind jedoch noch keine Berechtigungen zugewiesen.
Bearbeiten eines Berechtigungssatzes	**1** Wählen Sie den zu ändernden Berechtigungssatz aus. Detaillierte Informationen zu diesem Berechtigungssatz werden rechts angezeigt. Wenn Sie einen Berechtigungssatz erstellt haben, ist dieser bereits ausgewählt. **2** Wählen Sie eine Kategorie von zu ändernden Berechtigungen aus, indem Sie in der Zeile dieser Kategorie auf **Bearbeiten** klicken. **3** Ändern Sie die Berechtigungen, und klicken Sie dann auf **Speichern**, um den geänderten Berechtigungssatz in die Datenbank zu übernehmen. Wenn Sie den Berechtigungssatz geändert haben, müssen Sie zum Abschluss nicht auf **Speichern** klicken. Die Änderungen werden direkt beim Ändern der jeweiligen Kategorie gespeichert. Zudem werden die vorgenommenen Änderungen sofort im System übernommen und gemäß Ihrer Richtlinienkonfiguration im restlichen Netzwerk verbreitet.
Kopieren eines Berechtigungssatzes	**1** Wählen Sie den Berechtigungssatz, den Sie duplizieren möchten, in der Liste **Berechtigungssätze** aus, und klicken Sie dann auf **Aktionen** | **Duplizieren**. **2** Geben Sie einen neuen Namen für den duplizierten Berechtigungssatz ein. In der Standardeinstellung wird der Hinweis (Kopie) an den vorhandenen Namen angehängt. Die Verwendung eines bereits vorhandenen Namens ist nicht zulässig. Jeder Berechtigungssatz muss einen eindeutigen Namen besitzen. **3** Klicken Sie auf **OK**. Der Berechtigungssatz ist jetzt dupliziert, in der Liste Berechtigungssätze ist jedoch immer noch das Original ausgewählt.

Aktion	Vorgehensweise
Löschen eines Berechtigungssatzes	1 Wählen Sie in der Liste **Berechtigungssätze** den Berechtigungssatz aus, den Sie löschen möchten. Detaillierte Informationen zu diesem Berechtigungssatz werden rechts angezeigt. 2 Klicken Sie auf **Aktionen** | **Löschen** und dann auf **OK**. Der Berechtigungssatz wird nun nicht mehr in der Liste Berechtigungssätze angezeigt.
Exportieren von Berechtigungssätzen	Klicken Sie auf **Alle exportieren**. Vom McAfee ePO-Server wird eine XML-Datei an Ihren Browser gesendet. Der nächste Schritt hängt von Ihren Browser-Einstellungen ab. Von den meisten Browsern werden Sie zum Speichern der Datei aufgefordert. Die XML-Datei enthält nur Rollen mit definierten Berechtigungsebenen. Wenn zum Beispiel ein bestimmter Berechtigungssatz nicht über Berechtigungen für Abfragen und Berichte verfügt, enthält die Datei keinen Eintrag.
Importieren von Berechtigungssätzen	1 Klicken Sie auf **Importieren**. 2 Klicken Sie auf **Durchsuchen**, und wählen Sie die XML-Datei aus, in der sich der zu importierende Berechtigungssatz befindet. 3 Wählen Sie anhand der entsprechenden Option aus, ob Sie Berechtigungssätze, die den gleichen Namen wie importierte Berechtigungssätze haben, beibehalten möchten oder nicht. Klicken Sie auf **OK**. Wenn von McAfee ePO in der angegebenen Datei kein gültiger Berechtigungssatz gefunden wird, wird eine Fehlermeldung angezeigt, und der Importvorgang wird angehalten. Die Berechtigungssätze werden zum Server hinzugefügt und in der Liste Berechtigungssätze angezeigt.

6 Repositories

Auf Repositories befinden sich Sicherheits-Software-Pakete sowie deren Aktualisierungen zur Verteilung an die verwalteten Systeme.

Sicherheits-Software ist nur so effektiv wie die zuletzt installierten Aktualisierungen. Wenn zum Beispiel die DAT-Dateien veraltet sind, kann die beste Antiviren-Software keine neuen Bedrohungen erkennen. Es ist wichtig, eine zuverlässige Aktualisierungsstrategie zu entwickeln, damit die Sicherheits-Software immer so aktuell wie möglich ist.

Die Repository-Architektur von ePolicy Orchestrator bietet die Flexibilität, die erforderlich ist, damit das Ausbringen und Aktualisieren von Software so einfach und automatisch erfolgen kann, wie dies die jeweilige Umgebung zulässt. Erstellen Sie nach dem Einrichten der Repository-Infrastruktur Aktualisierungs-Tasks, die bestimmen, wie, wo und wann Ihre Software aktualisiert wird.

Inhalt

- *Repository-Typen und ihre Funktion*
- *Zusammenarbeit von Repositories*
- *Erstmaliges Einrichten von Repositories*
- *Verwalten von Quellsites und alternativen Sites*
- *Sicherstellen des Zugriffs auf die Quellsite*
- *Konfigurieren von Einstellungen für globale Aktualisierungen*
- *Konfigurieren von Agenten-Richtlinien zum Verwenden eines verteilten Repositorys*
- *Verwenden von SuperAgents als verteilte Repositories*
- *Erstellen und Konfigurieren von Repositories auf FTP- oder HTTP-Servern und UNC-Freigaben*
- *Verwenden von UNC-Freigaben als verteilte Repositories*
- *Verwenden von lokalen verteilten Repositories, die nicht verwaltet werden*
- *Arbeiten mit den Repository-Listen-Dateien*
- *Abruf-Tasks*
- *Replizierungs-Tasks*
- *Repository-Auswahl*

Repository-Typen und ihre Funktion

In McAfee ePO werden verschiedene Typen von Repositories bereitgestellt, mit denen Sie eine robuste Infrastruktur für Aktualisierungen aufbauen können.

Dank dieser Repositories können Sie ganz flexibel eine Aktualisierungsstrategie entwickeln, um Ihre Systeme immer auf dem aktuellen Stand zu halten.

Master-Repository

Im Master-Repository werden die neuesten Versionen der Sicherheits-Software und Aktualisierungen für die Umgebung verwaltet. Dieses Repository stellt die Quelle für den Rest der Umgebung dar.

Standardmäßig werden in McAfee ePO die Proxy-Einstellungen von Microsoft Internet Explorer verwendet.

Verteilte Repositories

In verteilten Repositories sind Kopien des Master-Repositorys gespeichert. Sie sollten verteilte Repositories verwenden und diese im gesamten Netzwerk verteilen. Durch diese Konfiguration können Sie sicherstellen, dass verwaltete Systeme auch dann aktualisiert werden, wenn insbesondere über langsame Verbindungen nur minimaler Netzwerkverkehr möglich ist.

Beim Aktualisieren des Master-Repositorys wird der Inhalt durch McAfee ePO in die verteilten Repositories repliziert.

Eine Replizierung kann bei folgenden Gelegenheiten stattfinden:

- Dies geschieht automatisch, wenn festgelegte Pakettypen in das Master-Repository eingecheckt werden und dabei die globale Aktualisierung aktiviert ist.
- Alternativ kann dies regelmäßig nach einem Zeitplan mithilfe von Replikations-Tasks geschehen.
- Sie können den Vorgang manuell ausführen, indem Sie den Task Jetzt replizieren ausführen.

Konfigurieren Sie verteilte Repositories nicht so, dass sie auf das gleiche Verzeichnis verweisen wie das Master-Repository. Dadurch würden die Dateien im Master-Repository gesperrt. Dadurch kann es zu Fehlern bei Abrufen und beim Einchecken von Paketen kommen, und das Master-Repository ist möglicherweise nicht mehr verwendbar.

In einem großen Unternehmen kann es mehrere Standorte geben, die über Leitungen mit begrenzter Bandbreite miteinander verbunden sind. Verteilte Repositories tragen dazu bei, den Aktualisierungsverkehr über Leitungen mit niedrigerer Bandbreite oder an Remote-Standorten mit zahlreichen Client-Systemen zu reduzieren. Wenn Sie an einem Remote-Standort ein verteiltes Repository erstellen und die Systeme an diesem Standort so konfigurieren, dass Aktualisierungen aus diesem verteilten Repository abgerufen werden, werden die Aktualisierungen nicht an alle Systeme am Remote-Standort einzeln, sondern nur einmal (an das verteilte Repository) über die langsame Verbindung kopiert.

Wenn die globale Aktualisierung aktiviert ist, werden verwaltete Systeme über verteilte Repositories automatisch aktualisiert, sobald bestimmte Aktualisierungen und Pakete in das Master-Repository eingecheckt wurden. Aktualisierungs-Tasks sind nicht erforderlich. Wenn Sie jedoch die automatische Aktualisierung verwenden möchten, müssen Sie in der Umgebung SuperAgents erstellen. Erstellen und konfigurieren Sie Repositories und die Aktualisierungs-Tasks.

Wenn verteilte Repositories so eingerichtet sind, dass nur ausgewählte Pakete repliziert werden, wird das neu eingecheckte Paket standardmäßig repliziert. Wenn ein neu eingechecktes Paket nicht repliziert werden soll, müssen Sie dessen Markierung in jedem verteilten Repository aufheben oder vor dem Einchecken des Pakets den Replikations-Task deaktivieren. Weitere Informationen finden Sie unter *Vermeiden der Replikation von ausgewählten Paketen* und *Deaktivieren der Replikation von ausgewählten Paketen*.

Quellsite

In der Quellsite werden alle Aktualisierungen für das Master-Repository bereitgestellt. Die standardmäßige Quellsite ist die McAfee-HTTP-Aktualisierungs-Site. Sie können die Quellsite jedoch auch ändern oder mehrere Quellsites konfigurieren.

Es wird empfohlen, die McAfee-HTTP- oder McAfee-FTP-Aktualisierungs-Site als Quellsite zu verwenden.

Quellsites sind nicht erforderlich. Sie können Aktualisierungen manuell herunterladen und in das Master-Repository einchecken. Wenn Sie eine Quellsite verwenden, wird dieser Vorgang jedoch automatisch durchgeführt.

McAfee veröffentlicht auf diesen Sites regelmäßig Software-Aktualisierungen. DAT-Dateien werden beispielsweise täglich veröffentlicht. Aktualisieren Sie Ihr Master-Repository mit Aktualisierungen, sobald diese verfügbar sind.

Kopieren Sie mithilfe von Abruf-Tasks Inhalte aus einer Quellsite in das Master-Repository.

Auf den McAfee-Aktualisierungssites werden nur Aktualisierungen von Erkennungsdefinitionen (DAT-Dateien) und Scan-Modulen sowie einige Sprachpakete bereitgestellt. Checken Sie alle anderen Pakete und Aktualisierungen, einschließlich Service Packs und Patches, manuell in das Master-Repository ein.

Alternative Site

Bei der alternativen Site handelt es sich um eine Quellsite, die als Sicherungsmöglichkeit dient. Von dieser Site können Aktualisierungen auf verwaltete Systeme abgerufen werden, wenn der Zugriff auf die gewohnten Repositories nicht möglich ist. Wenn zum Beispiel das Netzwerk ausfällt oder ein Virus ausbricht, sind die standardmäßigen Speicherorte in einigen Fällen nur noch schwierig erreichbar. Mithilfe alternativer Sites können verwaltete Systeme auf dem aktuellen Stand gehalten werden. Standardmäßig ist die alternative Site die McAfee-HTTP-Aktualisierungs-Site. Sie können nur eine alternative Site aktivieren.

Wenn auf verwalteten Systemen ein Proxy-Server für den Zugriff auf das Internet verwendet wird, konfigurieren Sie für diese Systeme die Einstellungen der Agentenrichtlinie so, dass der Zugriff auf diese alternative Site über Proxy-Server erfolgt.

Typen verteilter Repositories

ePolicy Orchestrator unterstützt vier Typen verteilter Repositories. Berücksichtigen Sie bei der Entscheidung, welcher Typ verteilter Repositories verwendet werden soll, Ihre Umgebung und Ihren Bedarf. Sie müssen sich nicht auf nur einen Typ beschränken. Je nach Netzwerk müssen Sie möglicherweise mehrere Typen verwenden.

SuperAgent-Repositories

Verwenden Sie Systeme mit SuperAgents als verteilte Repositories. SuperAgent-Repositories weisen gegenüber anderen Typen verteilter Repositories einige Vorteile auf:

- Ordnerpfade werden auf dem Hostsystem automatisch erstellt, bevor das Repository zur Repository-Liste hinzugefügt wird.
- Für SuperAgent-Repositories müssen keine Anmeldeinformationen für Replizierung oder Aktualisierung angegeben werden – die Kontoberechtigungen werden erstellt, wenn der Agent in einen SuperAgent konvertiert wird.

Damit die SuperAgent-Reaktivierung funktioniert, muss sich in jedem Übertragungssegment ein SuperAgent befinden. Für das SuperAgent-Repository ist dies dagegen nicht notwendig. Verwaltete Systeme müssen nur auf das System zugreifen können, auf dem sich das Repository befindet.

FTP-Repositories

Sie können ein verteiltes Repository auf einem FTP-Server speichern. Verwenden Sie eine FTP-Server-Software (z. B. die Microsoft-Internetinformationsdienste, IIS), um einen neuen Ordner und ein neues Siteverzeichnis für das verteilte Repository zu erstellen. Ausführliche Informationen hierzu finden Sie in der Dokumentation zum Web-Server.

HTTP-Repositories

Sie können ein verteiltes Repository auf einem HTTP-Server speichern. Verwenden Sie eine HTTP-Server-Software (z. B. Microsoft IIS), um einen neuen Ordner und ein neues Siteverzeichnis für das verteilte Repository zu erstellen. Ausführliche Informationen hierzu finden Sie in der Dokumentation zum Web-Server.

UNC-Freigabe-Repositories

Sie können einen freigegebenen UNC-Ordner erstellen, um ein verteiltes Repository auf einem vorhandenen Server zu speichern. Sie müssen den Ordner im gesamten Netzwerk freigeben, damit Ihr McAfee ePO-Server Dateien in diesen Ordner kopieren kann und Agenten für Aktualisierungen darauf zugreifen können.

Um auf den Ordner zugreifen zu können, müssen die richtigen Berechtigungen festgelegt sein.

Nicht verwaltete Repositories

Wenn Sie keine verwalteten verteilten Repositories verwenden können, können ePolicy Orchestrator-Administratoren verteilte Repositories erstellen und verwalten, die nicht von ePolicy Orchestrator verwaltet werden.

Wenn ein verteiltes Repository nicht von ePolicy Orchestrator verwaltet wird, muss ein lokaler Administrator die verteilten Dateien manuell auf dem aktuellen Stand halten.

Nachdem das verteilte Repository erstellt wurde, können Sie mit ePolicy Orchestrator verwaltete Systeme einer bestimmten Systemstrukturgruppe so konfigurieren, dass sie von dort Aktualisierungen abrufen.

Weitere Informationen zur Konfiguration von nicht verwalteten Systemen für die Verwendung mit ePO finden Sie unter *Aktivieren des Agenten auf nicht verwalteten McAfee-Produkten*.

Sie sollten alle verteilten Repositories über ePolicy Orchestrator verwalten. Dadurch und durch den häufigen Einsatz von globaler Aktualisierung oder geplanten Replizierungs-Tasks wird die Aktualität Ihrer verwalteten Umgebung gewährleistet. Nicht verwaltete verteilte Repositories sollten Sie nur dann verwenden, wenn verwaltete verteilte Repositories in Ihrem Netzwerk oder laut den Richtlinien Ihres Unternehmens nicht zulässig sind.

Repository-Zweige und ihre Verwendung

Mithilfe der drei ePolicy Orchestrator-Repository-Zweige können Sie bis zu drei Versionen der Pakete im Master-Repository und in den verteilten Repositories führen.

Die Repository-Zweige heißen Aktuell, Vorherige und Test. Standardmäßig wird in ePolicy Orchestrator nur der Zweig Aktuell verwendet. Sie können Zweige festlegen, wenn Sie Pakete zum Master-Repository hinzufügen. Außerdem können Sie Zweige festlegen, wenn Sie Aktualisierungs- und Bereitstellungs-Tasks durchführen oder planen, um verschiedene Versionen an unterschiedliche Punkte im Netzwerk zu verteilen.

Mit Aktualisierungs-Tasks können Aktualisierungen aus allen Zweigen des Repositorys abgerufen werden. Beim Einchecken von Paketen in das Master-Repository müssen Sie jedoch einen anderen Zweig als Aktuell auswählen. Falls nur der Zweig Aktuell konfiguriert ist, wird die Option zum Auswählen eines anderen Zweigs nicht angezeigt.

Um die Zweige Test und Vorherige für andere Pakete als Aktualisierungen verwenden zu können, müssen Sie die entsprechenden Server-Einstellungen für Repository-Pakete konfigurieren. Mit den Agenten-Versionen 3.6 und niedriger können nur Aktualisierungspakete aus den Zweigen Test und Vorherige abgerufen werden.

Zweig Aktuell

Der Zweig Aktuell ist der Repository-Hauptzweig für die neuesten Pakete und Aktualisierungen. Sofern keine Unterstützung für andere Zweige aktiviert ist, können Produktbereitstellungspakete nur zum Zweig Aktuell hinzugefügt werden.

Zweig Test

Es kann sinnvoll sein, neue DAT- und Scan-Modul-Aktualisierungen vor ihrer Bereitstellung im gesamten Unternehmen mit einer kleinen Anzahl von Netzwerksegmenten oder Systemen zu testen. Geben Sie den Zweig Test an, wenn Sie neue DAT- und Scan-Modul-Dateien in das Master-Repository einchecken, und stellen Sie sie dann auf einer kleinen Anzahl von Testsystemen bereit. Wenn Sie die Testsysteme mehrere Stunden lang überwacht haben, können Sie die neuen DAT-Dateien zum Zweig Aktuell hinzufügen und im gesamten Unternehmen bereitstellen.

Zweig Vorherige

Verwenden Sie den Zweig "Vorherige", um die vorherigen DAT- und Scan-Modul-Dateien zu sichern und zu speichern, bevor Sie neue zum Zweig Aktuell hinzufügen. Falls es in der Umgebung zu Problemen mit den neuen DAT- oder Scan-Modul-Dateien kommen sollte, können Sie die Kopie der vorherigen Version bei Bedarf erneut auf den Systemen bereitstellen. In ePolicy Orchestrator wird nur die neueste vorherige Version der einzelnen Dateitypen gespeichert.

Sie können den Zweig Vorherige auffüllen, indem Sie beim Hinzufügen neuer Pakete zum **Master-Repository** die Option Vorhandenes Paket in den Zweig "Vorherige" verschieben auswählen. Die Option ist verfügbar, wenn Sie Aktualisierungen von einer Quellsite abrufen und wenn Sie Pakete manuell in den Zweig Aktuell einchecken.

Repository-Listendateien

Die Repository-Listendateien (`(SiteList.xml` und `SiteMgr.xml`) enthalten die Namen aller Repositories, die Sie verwalten.

Die Repository-Liste enthält den Speicherort und die verschlüsselten Netzwerk-Anmeldeinformationen, die von verwalteten Systemen verwendet werden, um das Repository auszuwählen und Aktualisierungen abzurufen. Die Repository-Listen werden während der Agent-Server-Kommunikation vom Server an McAfee Agent gesendet.

Bei Bedarf können Sie die Repository-Liste in externe Dateien exportieren `(SiteList.xml` oder `SiteMgr.xml`). Die beiden Dateien werden zu unterschiedlichen Zwecken verwendet:

Datei **`SiteList.xml`**

- Importieren in McAfee Agent während der Installation

Datei **`SiteMgr.xml`**

- Sichern und Wiederherstellen verteilter Repositories und Quellsites, wenn der Server neu installiert werden muss
- Importieren der verteilten Repositories und Quellsites aus einer vorherigen Installation von McAfee ePO

Zusammenarbeit von Repositories

Die Repositories in Ihrer Umgebung arbeiten zusammen, um Aktualisierungen und Software auf die verwalteten Systeme zu übertragen. Je nach der Größe und geografischen Verteilung Ihres Netzwerks benötigen Sie möglicherweise verteilte Repositories.

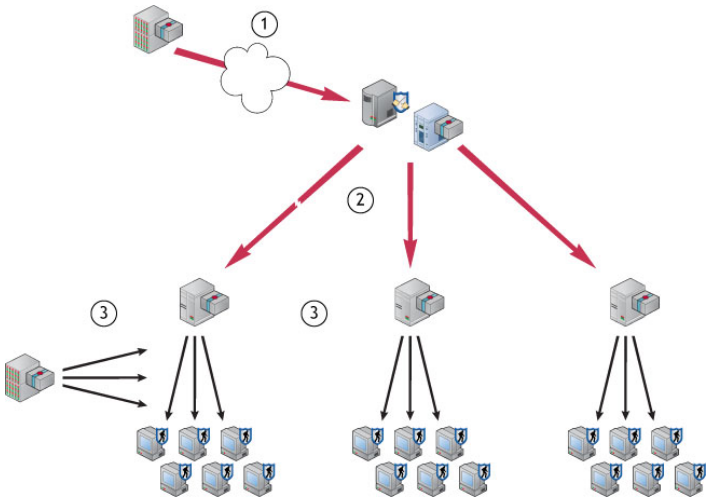


Abbildung 6-1 Sites und Repositories, die Pakete an Systeme verteilen

1 Es werden regelmäßig aktualisierte DAT- und Scan-Modul-Dateien aus der Quellsite in das Master-Repository abgerufen.

2 Die Pakete werden vom Master-Repository in verteilte Repositories im Netzwerk repliziert.

3 Die verwalteten Systeme im Netzwerk rufen Aktualisierungen aus einem verteilten Repository ab. Wenn verwaltete Systeme nicht auf verteilte Repositories oder das Master-Repository zugreifen können, rufen sie Aktualisierungen aus der alternativen Site ab.

Erstmaliges Einrichten von Repositories

Gehen Sie wie nachfolgend allgemein beschrieben vor, wenn Sie Repositories zum ersten Mal erstellen.

1 Entscheiden Sie, welche Repository-Typen verwendet werden und wo sich diese befinden sollen.

2 Erstellen Sie die Repositories, und füllen Sie sie auf.

Verwalten von Quellsites und alternativen Sites

In den Server-Einstellungen können Sie die standardmäßigen Quellsites und alternativen Sites ändern. So können Sie beispielsweise Einstellungen bearbeiten, vorhandene Quellsites und alternative Sites löschen oder zwischen diesen wechseln.

Um eine Quellsite oder alternative Site definieren, ändern oder löschen zu können, müssen Sie als Administrator angemeldet sein oder die entsprechenden Berechtigungen besitzen.

McAfee empfiehlt, die standardmäßigen Quellsites und alternativen Sites zu verwenden. Wenn Sie hierfür andere Sites benötigen, können Sie neue erstellen.

Aufgaben

- *Erstellen von Quellsites* auf Seite 71
  Erstellen Sie unter Server-Einstellungen eine neue Quellsite.
- *Wechseln zwischen Quellsites und alternativen Sites* auf Seite 72
  Mit den Server-Einstellungen können Sie die Quellsites und alternativen Sites ändern.
- *Bearbeiten von Quellsites und alternativen Sites* auf Seite 72
  Unter Server-Einstellungen können Sie die Einstellungen (wie URL-Adresse, Portnummer, Authentifizierungs-Anmeldeinformationen zum Herunterladen) von Quellsites oder alternativen Sites bearbeiten.
- *Löschen von Quellsites oder Deaktivieren alternativer Sites* auf Seite 73
  Wenn eine Quellsite oder eine alternative Site nicht mehr benötigt wird, können Sie sie löschen oder deaktivieren.

Erstellen von Quellsites

Erstellen Sie unter Server-Einstellungen eine neue Quellsite.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, und wählen Sie dann **Quellsites** aus.

2 Klicken Sie auf **Quellsite hinzufügen**. Der Assistent Quellsite-Generator wird angezeigt.

3 Geben Sie auf der Seite Beschreibung einen eindeutigen Repository-Namen ein, wählen Sie **HTTP**, **UNC** oder **FTP** aus, und klicken Sie dann auf **Weiter**.

4 Geben Sie auf der Seite Server die Informationen zur Web-Adresse und zum Port der Site an, und klicken Sie dann auf **Weiter**.

Bei HTTP- oder FTP-Servern:

- Wählen Sie in der Dropdown-Liste **URL** als Typ der Server-Adresse den Eintrag **DNS-Name**, **IPv4** oder **IPv6** aus, und geben Sie dann die Adresse ein.

Option	Definition
DNS-Name	Gibt den DNS-Namen des Servers an.
IPv4	Gibt die IPv4-Adresse des Servers an.
IPv6	Gibt die IPv6-Adresse des Servers an.

- Geben Sie die Portnummer des Servers ein: Bei FTP ist dies standardmäßig 21. Bei HTTP ist dies 80.

Bei UNC-Servern:

- Geben Sie den Pfad zu dem Netzwerkverzeichnis ein, in dem sich das Repository befindet. Verwenden Sie das folgende Format: `\\<COMPUTER>\<ORDNER>`.

5 Geben Sie auf der Seite Anmeldeinformationen die **Download-Anmeldeinformationen** an, die von verwalteten Systemen für Verbindungen mit diesem Repository verwendet werden.

Verwenden Sie Anmeldeinformationen, die nur schreibgeschützten Zugriff auf den HTTP-Server, den FTP-Server oder die UNC-Freigabe mit dem Repository gewähren.

Bei HTTP- oder FTP-Servern:

- Aktivieren Sie **Anonym**, wenn ein unbekanntes Benutzerkonto verwendet werden soll.
- Wenn beim Server eine Authentifizierung erforderlich ist, aktivieren Sie **FTP-Authentifizierung** oder **HTTP-Authentifizierung**, und geben Sie dann die Benutzerkontoinformationen ein.

Bei UNC-Servern:

- Geben Sie die Domäne und die Benutzerkontoinformationen ein.

6 Klicken Sie auf **Anmeldeinformationen testen**. Nach wenigen Sekunden wird eine Meldung mit der Bestätigung angezeigt, dass über Systeme, von denen die Authentifizierungsinformationen verwendet werden, auf die Site zugegriffen werden kann. Wenn die Anmeldeinformationen falsch sind, überprüfen Sie Folgendes:

- Benutzername und Kennwort
- URL-Adresse oder Pfad im vorherigen Fenster des Assistenten
- HTTP-, FTP oder UNC-Site des Systems

7 Klicken Sie auf **Weiter**.

8 Überprüfen Sie die Angaben auf der Seite Übersicht, und klicken Sie dann auf **Speichern**, um die Site zur Liste hinzuzufügen.

Wechseln zwischen Quellsites und alternativen Sites

Mit den Server-Einstellungen können Sie die Quellsites und alternativen Sites ändern.

Je nach Ihrer Netzwerkkonfiguration möchten Sie vielleicht zwischen Quellsite und alternativer Site umschalten, wenn Sie feststellen, dass die HTTP- oder die FTP-Aktualisierung besser funktioniert.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**.

2 Wählen Sie **Quellsites** aus, und klicken Sie dann auf **Bearbeiten**. Die Seite Quellsites bearbeiten wird angezeigt.

3 Suchen Sie in der Liste die Site, die Sie als alternative Site festlegen möchten, und klicken Sie dann auf **Alternative aktivieren**.

Bearbeiten von Quellsites und alternativen Sites

Unter Server-Einstellungen können Sie die Einstellungen (wie URL-Adresse, Portnummer, Authentifizierungs-Anmeldeinformationen zum Herunterladen) von Quellsites oder alternativen Sites bearbeiten.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**.

2 Wählen Sie **Quellsites** aus, und klicken Sie dann auf **Bearbeiten**. Die Seite Quellsites bearbeiten wird angezeigt.

3 Suchen Sie die Site in der Liste, und klicken Sie auf den Namen der Site.

Der Assistent für den Quellsite-Generator wird angezeigt.

4 Bearbeiten Sie die im Assistenten angezeigten Einstellungen nach Bedarf, und klicken Sie dann auf **Speichern**.

Löschen von Quellsites oder Deaktivieren alternativer Sites

Wenn eine Quellsite oder eine alternative Site nicht mehr benötigt wird, können Sie sie löschen oder deaktivieren.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**.

2 Wählen Sie **Quellsites** aus, und klicken Sie dann auf **Bearbeiten**. Die Seite Quellsites bearbeiten wird angezeigt.

3 Klicken Sie neben der erforderlichen Quellsite auf **Löschen**. Das Dialogfeld Quellsite löschen wird angezeigt.

4 Klicken Sie auf **OK**.

Die Site wird von der Seite Quellsites gelöscht.

Sicherstellen des Zugriffs auf die Quellsite

Stellen Sie sicher, dass für das ePolicy Orchestrator-Master-Repository und die verwalteten Systeme eine Internetverbindung hergestellt werden kann, wenn die Sites McAfeeHttp und McAfeeFTP als Quellsites und alternative Sites verwendet werden.

In diesem Abschnitt werden die erforderlichen Tasks zur Konfiguration der Verbindung beschrieben, die vom ePolicy Orchestrator-Master-Repository und McAfee Agent direkt oder über einen Proxy zur Download-Site hergestellt werden kann. Standardmäßig ist **Keinen Proxy verwenden** ausgewählt.

Aufgaben

- *Konfigurieren von Proxyeinstellungen* auf Seite 73
  Wenn Sie Ihre Repositories aktualisieren möchten, konfigurieren Sie die Proxyeinstellungen zum Abrufen der DAT-Dateien.
- *Konfigurieren von Proxyeinstellungen für McAfee Agent* auf Seite 74
  Sie können die Proxyeinstellungen konfigurieren, mit denen McAfee Agent eine Verbindung zur Download-Website herstellt.

Konfigurieren von Proxyeinstellungen

Wenn Sie Ihre Repositories aktualisieren möchten, konfigurieren Sie die Proxyeinstellungen zum Abrufen der DAT-Dateien.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**.

2 Wählen Sie in der Liste Einstellungskategorien die Option **Proxyeinstellungen** aus, und klicken Sie dann auf **Bearbeiten**.

3 Wählen Sie **Proxyeinstellungen manuell konfigurieren** aus.

   a Wählen Sie neben Proxyserver-Einstellungen aus, ob ein Proxyserver für die gesamte Kommunikation oder unterschiedliche Proxyserver als HTTP- und FTP-Proxyserver verwendet werden sollen. Geben Sie die IP-Adresse oder den vollqualifizierten Domänennamen und die Portnummer des Proxyservers ein.

   Wenn Sie die standardmäßigen Quell- und alternativen Sites verwenden oder andere HTTP-Quellsites und alternativen FTP-Sites konfigurieren, geben Sie hier sowohl die HTTP- als auch die FTP-Proxy-Authentifizierungsinformationen an.

   b Nehmen Sie neben Proxyauthentifizierung die entsprechenden Einstellungen vor, je nach dem, ob Sie Aktualisierungen aus HTTP-, aus FTP-Repositories oder aus beiden abrufen möchten.

   c Aktivieren Sie neben Ausschlüsse die Option **Lokale Adressen umgehen**, und legen Sie dann alle verteilten Repositories fest, zu denen für den Server eine direkte Verbindung hergestellt werden kann. Geben Sie dazu die IP-Adressen oder die vollqualifizierten Domänennamen dieser Systeme ein (getrennt durch ein Semikolon).

   d Aktivieren Sie neben Ausschlüsse die Option **Lokale Adressen umgehen**, und legen Sie dann alle verteilten Repositories fest, zu denen für den Server eine direkte Verbindung hergestellt werden kann. Geben Sie dazu die IP-Adressen oder die vollqualifizierten Domänennamen dieser Systeme ein (getrennt durch ein Semikolon).

4 Klicken Sie auf **Speichern**.

Konfigurieren von Proxyeinstellungen für McAfee Agent

Sie können die Proxyeinstellungen konfigurieren, mit denen McAfee Agent eine Verbindung zur Download-Website herstellt.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Richtlinie** | **Richtlinienkatalog**, und wählen Sie dann in der Dropdown-Liste **Produkt** den Eintrag **McAfee Agent** und in der Dropdown-Liste **Kategorie** den Eintrag **Repository** aus.

   Eine Liste mit den für den McAfee ePO-Server konfigurierten Agenten wird angezeigt.

2 Klicken Sie für den Agenten **My Default** auf **Einstellungen bearbeiten**.

   Die Seite Einstellungen bearbeiten für den Agenten My Default wird angezeigt.

3 Klicken Sie auf die Registerkarte **Proxy**.

   Die Seite Proxyeinstellungen wird angezeigt.

4 Wählen Sie die Option **Internet Explorer-Einstellungen verwenden (nur Windows)** für Windows-Systeme und bei Bedarf **Konfigurieren von Proxyeinstellungen durch Benutzer zulassen** aus.

   Internet Explorer kann auf mehrere Arten für die Verwendung mit Proxies konfiguriert werden. McAfee stellt Anweisungen für die Konfiguration und Verwendung von McAfee-Produkten, nicht jedoch für Produkte von anderen Anbietern als McAfee bereit. Weitere Informationen über das Konfigurieren von Proxyeinstellungen finden Sie in der Hilfe zu Internet Explorer und unter http://support.microsoft.com/kb/226473.

5 Wählen Sie **Proxyeinstellungen manuell konfigurieren** aus, um die Proxyeinstellungen für den Agenten manuell zu konfigurieren.

6 Geben Sie die IP-Adresse oder den vollqualifizierten Domänennamen und die Portnummer der HTTP- oder FTP-Quelle ein, von der der Agent Aktualisierungen abruft. Aktivieren Sie **Diese Einstellungen für alle Proxytypen verwenden**, um diese Einstellungen als Standardeinstellung für alle Proxytypen festzulegen.

7 Wählen Sie **Ausnahmen festlegen** aus, um Systeme zu kennzeichnen, die keinen Zugriff auf den Proxy benötigen. Verwenden Sie ein Semikolon, um Ausnahmen voneinander zu trennen.

8 Aktivieren Sie **HTTP-Proxyauthentifizierung verwenden** oder **FTP-Proxyauthentifizierung verwenden**, und geben Sie dann einen Benutzernamen und Anmeldeinformationen an.

9 Klicken Sie auf **Speichern**.

Konfigurieren von Einstellungen für globale Aktualisierungen

Mit globalen Aktualisierungen können Sie die Repository-Replikation im Netzwerk automatisieren. Mit der Server-Einstellung Globale Aktualisierung können Sie die Inhalte konfigurieren, die bei einer globalen Aktualisierung an Repositories verteilt werden.

Globale Aktualisierungen sind standardmäßig deaktiviert. McAfee empfiehlt jedoch, dass Sie diese Aktualisierungen aktivieren und im Rahmen Ihrer Aktualisierungsstrategie nutzen. Sie können ein Zufallsintervall und Pakettypen angeben, die während der Aktualisierung verteilt werden sollen. Das Zufallsintervall gibt die Zeitspanne an, in der alle Systeme aktualisiert werden. Innerhalb dieses angegebenen Intervalls werden die Systeme auf Zufallsbasis aktualisiert.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste **Einstellungskategorien** den Eintrag Globale Aktualisierung aus, und klicken Sie dann auf **Bearbeiten**.

2 Legen Sie für den Status **Aktiviert** fest, und geben Sie ein **Zufallsintervall** zwischen 0 und 32.767 Minuten an.

3 Geben Sie an, welche **Pakettypen** in den globalen Aktualisierungen enthalten sein sollen:

- **Alle Pakete** – Bei Auswahl dieser Option werden alle Signaturen und Scan-Module sowie alle Patches und Service Packs in die globalen Aktualisierungen eingeschlossen.
- **Ausgewählte Pakete** – Bei dieser Option können Sie die in globalen Aktualisierungen eingeschlossenen Signaturen und Scan-Module sowie Patches und Service Packs begrenzen.

Wenn Sie die globale Aktualisierung verwenden, empfiehlt McAfee, einen regelmäßigen Abruf-Task (zum Aktualisieren des Master-Repositorys) für einen Zeitpunkt mit geringem Netzwerkverkehr zu planen. Die globale Aktualisierung ist zwar die schnellste Aktualisierungsmethode, verursacht dabei jedoch verstärkten Netzwerkverkehr. Weitere Informationen zum Durchführen globaler Aktualisierungen finden Sie in *Globale Aktualisierung* unter *Bereitstellen von Produkten und Aktualisierungen*.

Konfigurieren von Agenten-Richtlinien zum Verwenden eines verteilten Repositorys

Sie können anpassen, wie Agenten verteilte Repositories zur Minimierung der Bandbreitennutzung auswählen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Richtlinie** | **Richtlinienkatalog**, und wählen Sie dann in der Dropdown-Liste **Produkt** den Eintrag **McAfee Agent** und in der Dropdown-Liste **Kategorie** den Eintrag **Repository** aus.

2 Klicken Sie auf die erforderliche vorhandene Agenten-Richtlinie.

3 Wählen Sie die Registerkarte Repositories aus.

4 Wählen Sie unter Repository-Listenauswahl entweder **Diese Repository-Liste verwenden** oder **Andere Repository-Liste verwenden** aus.

5 Geben Sie unter Repository auswählen nach die Methode an, die zum Sortieren von Repositories verwendet werden soll:

- **Ping-Zeit** – Sendet einen ICMP-Ping an die (nach dem Subnetzwert) nächstgelegenen fünf Repositories und sortiert diese nach der Reaktionszeit.
- **Subnetzentfernung** – Vergleicht die IP-Adressen von Client-Systemen und sämtlichen Repositories und sortiert Repositories danach, wie genau die Bits übereinstimmen. Je mehr die IP-Adressen übereinstimmen, desto höher wird das Repository in der Liste eingestuft.

  Bei Bedarf können Sie die **Maximale Anzahl der Hops** festlegen.

- **Reihenfolge in der Repository-Liste verwenden** – Wählt Repositories auf Grundlage ihrer Reihenfolge in der Liste aus.

6 In der Repository-Liste können Sie Repositories deaktivieren, indem Sie im Feld **Aktionen** des zu deaktivierenden Repositorys auf **Deaktivieren** klicken.

7 Klicken Sie in der Repository-Liste auf **Zum Anfang** oder **Zum Ende**, um die Reihenfolge festzulegen, in der verteilte Repositories von Client-Systemen ausgewählt werden sollen.

8 Klicken Sie abschließend auf **Speichern**.

Verwenden von SuperAgents als verteilte Repositories

Sie können auf Systemen, auf denen sich SuperAgents befinden, verteilte Repositories erstellen und konfigurieren. Mithilfe von SuperAgents kann der Netzwerkdatenverkehr minimiert werden.

Damit ein Agent in einen SuperAgent umgewandelt werden kann, muss er zu einer Windows-Domäne gehören.

Aufgaben

- *Erstellen von verteilten SuperAgent-Repositories* auf Seite 77
  Zum Erstellen eines SuperAgent-Repositorys muss auf dem SuperAgent-System ein McAfee Agent installiert sein und ausgeführt werden. Sie sollten SuperAgent-Repositories mit aktivierter globaler Aktualisierung verwenden.
- *Replizieren von Paketen in SuperAgent-Repositories* auf Seite 78
  Sie können auswählen, welche Repository-spezifischen Pakete in verteilte Repositories repliziert werden.
- *Löschen von verteilten SuperAgent-Repositories* auf Seite 78
  Sie können verteilte SuperAgent-Repositories aus dem Hostsystem und der Repository-Liste (SITELIST.XML) entfernen. Neue Konfigurationen werden während des nächsten Agent-zu-Server-Kommunikationsintervalls wirksam.

Erstellen von verteilten SuperAgent-Repositories

Zum Erstellen eines SuperAgent-Repositorys muss auf dem SuperAgent-System ein McAfee Agent installiert sein und ausgeführt werden. Sie sollten SuperAgent-Repositories mit aktivierter globaler Aktualisierung verwenden.

Bei dieser Vorgehensweise wird davon ausgegangen, dass Sie wissen, wo sich die SuperAgent-Systeme in der Systemstruktur befinden. Sie sollten ein SuperAgent-Tag erstellen, damit Sie die SuperAgent-Systeme mithilfe der Seite Tag-Katalog oder durch Ausführen einer Abfrage leicht finden können.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie in der ePolicy Orchestrator-Konsole auf **Menü** | **Richtlinie** | **Richtlinienkatalog**, und wählen Sie dann in der Dropdown-Liste **Produkt** den Eintrag **McAfee Agent** und in der Dropdown-Liste Kategorie den Eintrag **Allgemein** aus.

   Es wird eine Liste mit den Richtlinien der Kategorie Allgemein angezeigt, die für Ihren McAfee ePO-Server zur Verfügung stehen.

2 Erstellen Sie eine neue Richtlinie, duplizieren Sie eine vorhandene Richtlinie, oder öffnen Sie eine vorhandene Richtlinie, die bereits auf Systeme mit einem SuperAgent angewendet wird, auf denen Sie SuperAgent-Repositories hosten möchten.

3 Wählen Sie die Registerkarte **Allgemein** aus, und vergewissern Sie sich, dass die Option **Agenten in SuperAgents konvertieren (nur Windows)** ausgewählt ist.

4 Aktivieren Sie **Systeme mit SuperAgents als verteilte Repositories verwenden**, und geben Sie dann einen Ordnerpfad als Speicherort für das Repository ein. Dies ist der Speicherort, in den das Master-Repository die Aktualisierungen während der Replizierung kopiert. Sie können einen Standardpfad von Windows verwenden, wie `C:\SuperAgent\Repo`.

   Alle angeforderten Dateien vom Agenten-System werden aus diesem Speicherort über den integrierten HTTP-Web-Server des Agenten übermittelt.

5 Klicken Sie auf **Speichern**.

6 Weisen Sie diese Richtlinie jedem System zu, das als Host für ein SuperAgent-Repository dienen soll.

Wenn sich der Agent das nächste Mal beim Server meldet, wird die neue Richtlinie abgerufen. Wenn Sie nicht bis zur nächsten Agent-zu-Server-Kommunikation warten möchten, können Sie eine Agenten-Reaktivierung an die Systeme senden. Beim Erstellen des verteilten Repositorys wird der angegebene Ordner auf dem System erstellt, falls dieser nicht bereits vorhanden ist.

Außerdem wird der Speicherort zur Repository-Liste der Datei `SITELIST.XML` hinzugefügt. Auf diese Weise kann die Site von Systemen in der verwalteten Umgebung zum Aktualisieren verwendet werden.

Replizieren von Paketen in SuperAgent-Repositories

Sie können auswählen, welche Repository-spezifischen Pakete in verteilte Repositories repliziert werden.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Software** | **Verteilte Repositories**.

Eine Liste aller verteilten Repositories wird angezeigt.

2 Suchen Sie das SuperAgent-Repository, und klicken Sie darauf.

Der Assistent Generator für verteilte Repositories wird geöffnet.

3 Wählen Sie auf der Seite **Pakettypen** die erforderlichen Pakettypen aus.

Achten Sie darauf, dass alle Pakete ausgewählt sind, die von den verwalteten Systemen benötigt werden, die dieses Repository verwenden. Verwaltete Systeme greifen für alle Pakete auf ein Repository zurück. Wenn ein erwarteter Pakettyp nicht vorhanden ist, kann der Task auf Systemen nicht ausgeführt werden. Diese Funktion stellt sicher, dass Pakete, die nur von wenigen Systemen verwendet werden, nicht in der gesamten Umgebung repliziert werden.

4 Klicken Sie auf **Speichern**.

Löschen von verteilten SuperAgent-Repositories

Sie können verteilte SuperAgent-Repositories aus dem Hostsystem und der Repository-Liste (SITELIST.XML) entfernen. Neue Konfigurationen werden während des nächsten Agent-zu-Server-Kommunikationsintervalls wirksam.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie in der ePolicy Orchestrator-Konsole auf **Menü** | **Richtlinie** | **Richtlinienkatalog**, und klicken Sie dann auf den Namen der SuperAgent-Richtlinie, die Sie ändern möchten.

2 Deaktivieren Sie auf der Registerkarte **Allgemein** die Option **Systeme mit SuperAgents als verteilte Repositories verwenden**, und klicken Sie dann auf **Speichern**.

Um eine begrenzte Anzahl vorhandener verteilter SuperAgent-Repositories zu löschen, duplizieren Sie die diesen Systemen zugewiesene McAfee Agent-Richtlinie, und deaktivieren Sie die Option **Systeme mit SuperAgents als verteilte Repositories verwenden**, bevor Sie sie speichern. Weisen Sie diese neue Richtlinie dann je nach Bedarf zu.

Das SuperAgent-Repository wird gelöscht und aus der Repository-Liste entfernt. Der Agent fungiert jedoch so lange als SuperAgent, bis die Option **Agenten in SuperAgents konvertieren (nur Windows)** deaktiviert wird. Agenten, die nach der Richtlinienänderungen keine neue Sitelist erhalten haben, beziehen ihre Aktualisierungen weiter von dem SuperAgent, der entfernt wurde.

Erstellen und Konfigurieren von Repositories auf FTP- oder HTTP-Servern und UNC-Freigaben

Sie können verteilte Repositories auf vorhandenen FTP- und HTTP-Servern oder UNC-Freigaben hosten. Ein dedizierter Server ist jedoch nicht erforderlich. Das System sollte robust genug sein, um die Lasten zu bewältigen, wenn verwaltete Systeme Verbindungen zum Abrufen von Aktualisierungen herstellen.

Aufgaben

- *Erstellen eines Ordnerspeicherorts* auf Seite 80
  Erstellen Sie den Ordner, der auf dem System mit dem verteilten Repository die Repository-Inhalte enthält. Die Vorgehensweise für UNC-Freigabe-Repositories ist dabei anders als für FTP- oder HTTP-Repositories.
- *Hinzufügen des verteilten Repositorys zu ePolicy Orchestrator* auf Seite 80
  Sie können einen Eintrag zur Repository-Liste hinzufügen und den Ordner angeben, der von dem neuen verteilten Repository verwendet wird.
- *Vermeiden der Replizierung von ausgewählten Paketen* auf Seite 82
  Wenn verteilte Repositories so eingerichtet sind, dass nur ausgewählte Pakete repliziert werden, wird Ihr neu eingecheckte Paket standardmäßig repliziert. Je nach Ihren Anforderungen in Bezug auf Tests und Überprüfungen möchten Sie möglicherweise vermeiden, dass bestimmte Pakete in Ihre verteilten Repositories repliziert werden.
- *Deaktivieren der Replizierung von ausgewählten Paketen* auf Seite 82
  Wenn verteilte Repositories so eingerichtet sind, dass nur ausgewählte Pakete repliziert werden, wird Ihr neu eingecheckte Paket standardmäßig repliziert. Falls Sie die bevorstehende Replizierung eines Pakets deaktivieren möchten, deaktivieren Sie den Replizierungs-Task, bevor Sie das Paket einchecken.
- *Aktivieren der Ordnerfreigabe für UNC- und HTTP-Repositories* auf Seite 83
  Bei einem verteilten HTTP- oder UNC-Repository müssen Sie den Ordner für die Freigabe im Netzwerk aktivieren, damit der McAfee ePO-Server Dateien in das Repository kopieren kann.
- *Bearbeiten von verteilten Repositories* auf Seite 83
  Bearbeiten Sie nach Bedarf die Konfigurations-, Authentifizierungs- und Paketauswahloptionen eines verteilten Repositorys.
- *Löschen von verteilten Repositories* auf Seite 83
  Sie können verteilte Repositories aus HTTP- und FTP-Servern oder UNC-Freigaben löschen. Bei diesem Vorgang werden auch die in den Repositories gespeicherten Inhalte gelöscht.

Erstellen eines Ordnerspeicherorts

Erstellen Sie den Ordner, der auf dem System mit dem verteilten Repository die Repository-Inhalte enthält. Die Vorgehensweise für UNC-Freigabe-Repositories ist dabei anders als für FTP- oder HTTP-Repositories.

- Für UNC-Freigabe-Repositories erstellen Sie den Ordner auf dem System und aktivieren die Freigabe.
- Für FTP- oder HTTP-Repositories können Sie Ihre vorhandene FTP- oder HTTP-Server-Software (z. B. die Microsoft-Internetinformationsdienste, IIS) verwenden, um einen neuen Ordner und ein neues Siteverzeichnis zu erstellen. Ausführliche Informationen hierzu finden Sie in der Dokumentation zum Web-Server.

Hinzufügen des verteilten Repositorys zu ePolicy Orchestrator

Sie können einen Eintrag zur Repository-Liste hinzufügen und den Ordner angeben, der von dem neuen verteilten Repository verwendet wird.

Konfigurieren Sie verteilte Repositories nicht so, dass sie auf dasselbe Verzeichnis verweisen wie Ihr Master-Repository. Ansonsten werden die Dateien auf dem Master-Repository durch Benutzer des verteilten Repositorys gesperrt, wodurch Abrufe und das Einchecken von Paketen fehlschlagen können und das Master-Repository nicht mehr verwendbar ist.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Software** | **Verteilte Repositories** und anschließend auf **Aktionen** | **Neues Repository**. Der Assistent **Generator für verteilte Repositories** wird geöffnet.

2 Geben Sie auf der Seite **Beschreibung** einen eindeutigen Namen ein, wählen Sie **HTTP**, **UNC** oder **FTP** aus, und klicken Sie dann auf **Weiter**. Bei dem Namen des Repositorys muss es sich nicht um den Namen des Systems handeln, das als Host für das Repository dient.

3 Konfigurieren Sie auf der Seite **Server** einen der folgenden **Server-Typen**:

Bei HTTP-Servern:

- Wählen Sie in der Liste **URL** als Typ der Server-Adresse den Eintrag **DNS-Name**, **IPv4** oder **IPv6** aus, und geben Sie dann die Adresse ein.

Option	Definition
DNS-Name	Gibt den DNS-Namen des Servers an.
IPv4	Gibt die IPv4-Adresse des Servers an.
IPv6	Gibt die IPv6-Adresse des Servers an.

- Geben Sie die Portnummer des Servers ein: Bei HTTP ist der Standardwert 80.
- Geben Sie den **UNC-Pfad für die Replizierung** für den HTTP-Ordner an.

Bei UNC-Servern:

- Geben Sie den Pfad zu dem Netzwerkverzeichnis ein, in dem sich das Repository befindet. Verwenden Sie das folgende Format: `\\<COMPUTER>\<ORDNER>`.

Bei FTP-Servern:

- Wählen Sie in der Liste **URL** als Typ der Server-Adresse den Eintrag **DNS-Name**, **IPv4** oder **IPv6** aus, und geben Sie dann die Adresse ein.

Option	Definition
DNS-Name	Gibt den DNS-Namen des Servers an.
IPv4	Gibt die IPv4-Adresse des Servers an.
IPv6	Gibt die IPv6-Adresse des Servers an.

- Geben Sie die Portnummer des Servers ein: Bei FTP ist der Standardwert 21.

4 Klicken Sie auf **Weiter**.

5 Gehen Sie auf der Seite **Anmeldeinformationen** wie folgt vor:

a Geben Sie die **Anmeldeinformationen zum Herunterladen** ein. Verwenden Sie Anmeldeinformationen, die nur schreibgeschützten Zugriff auf den HTTP-Server, FTP-Server oder die UNC-Freigabe mit dem Repository gewähren.

Bei HTTP- oder FTP-Servern:

- Aktivieren Sie **Anonym**, wenn ein unbekanntes Benutzerkonto verwendet werden soll.
- Wenn beim Server eine Authentifizierung erforderlich ist, aktivieren Sie **FTP-Authentifizierung** oder **HTTP-Authentifizierung**, und Sie geben dann die Benutzerkontoinformationen ein.

Bei UNC-Servern:

- Wählen Sie **Anmeldeinformationen des angemeldeten Kontos verwenden** aus, um die Anmeldeinformationen des momentan angemeldeten Benutzers zu verwenden.
- Wählen Sie **Geben Sie die Anmeldeinformationen zum Herunterladen ein** aus, und geben Sie die Domänen- und Benutzerkontoinformationen ein.

b Klicken Sie auf **Anmeldeinformationen testen**. Nach wenigen Sekunden wird eine Meldung mit der Bestätigung angezeigt, dass Systeme, die die Authentifizierungsinformationen verwenden, auf die Site zugreifen können. Wenn die Anmeldeinformationen falsch sind, überprüfen Sie Folgendes:

- Benutzername und Kennwort
- URL-Adresse oder Pfad im vorherigen Fenster des Assistenten
- HTTP-, FTP oder UNC-Site des Systems

6 Geben Sie die **Anmeldeinformationen zum Replizieren** ein.

Der Server verwendet diese Anmeldeinformationen beim Replizieren von DAT-Dateien, Scan-Modul-Dateien oder anderen Produktaktualisierungen aus dem Master-Repository in das verteilte Repository. Diese Anmeldeinformationen müssen sowohl Lese- als auch Schreibberechtigungen für das verteilte Repository implizieren.

- Wenn Sie **FTP** ausgewählt haben, geben Sie die Benutzerkontoinformationen ein.
- Wenn Sie **HTTP** oder **UNC** ausgewählt haben, geben Sie die Domänen- und Benutzerkontoinformationen ein.
- Klicken Sie auf **Anmeldeinformationen testen**. Nach wenigen Sekunden wird eine Meldung mit der Bestätigung angezeigt, dass Systeme, die die Authentifizierungsinformationen verwenden, auf

die Site zugreifen können. Wenn die Anmeldeinformationen falsch sind, überprüfen Sie Folgendes:

- Benutzername und Kennwort
- URL-Adresse oder Pfad im vorherigen Fenster des Assistenten
- HTTP-, FTP oder UNC-Site des Systems

7 Klicken Sie auf **Weiter**. Die Seite **Pakettypen** wird angezeigt.

8 Legen Sie fest, ob alle oder nur ausgewählte Pakete in dieses verteilte Repository repliziert werden sollen, und klicken Sie dann auf **Weiter**.

- Wenn Sie die Option **Ausgewählte Pakete** ausgewählt haben, müssen Sie die zu replizierenden **Signaturen und Scan-Module** sowie **Produkte, Patches, Service Packs etc.** manuell auswählen.
- Wählen Sie optional **Alte DAT-Dateien replizieren** aus.

Achten Sie darauf, dass alle Pakete aktiviert sind, die von den verwalteten Systemen benötigt werden, die dieses Repository verwenden. Verwaltete Systeme greifen für alle Pakete auf ein Repository zurück. Wenn ein erforderlicher Pakettyp im Repository nicht vorhanden ist, kann der Task nicht ausgeführt werden. Diese Funktion stellt sicher, dass Pakete, die nur von wenigen Systemen verwendet werden, nicht in der gesamten Umgebung repliziert werden.

9 Überprüfen Sie die Angaben auf der Seite **Zusammenfassung**, und klicken Sie dann auf **Speichern**, um das Repository hinzuzufügen. ePolicy Orchestrator fügt das neue verteilte Repository zu seiner Datenbank hinzu.

Vermeiden der Replizierung von ausgewählten Paketen

Wenn verteilte Repositories so eingerichtet sind, dass nur ausgewählte Pakete repliziert werden, wird Ihr neu eingechecktes Paket standardmäßig repliziert. Je nach Ihren Anforderungen in Bezug auf Tests und Überprüfungen möchten Sie möglicherweise vermeiden, dass bestimmte Pakete in Ihre verteilten Repositories repliziert werden.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Software** | **Verteilte Repositories** und anschließend auf ein Repository. Der Assistent Generator für verteilte Repositories wird geöffnet.

2 Deaktivieren Sie auf der Seite Pakettypen das Paket, dessen Replizierung Sie vermeiden möchten.

3 Klicken Sie auf **Speichern**.

Deaktivieren der Replizierung von ausgewählten Paketen

Wenn verteilte Repositories so eingerichtet sind, dass nur ausgewählte Pakete repliziert werden, wird Ihr neu eingechecktes Paket standardmäßig repliziert. Falls Sie die bevorstehende Replizierung eines Pakets deaktivieren möchten, deaktivieren Sie den Replizierungs-Task, bevor Sie das Paket einchecken.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Automatisierung** | **Server-Tasks**, und wählen Sie dann neben einem Replizierungs-Server-Task die Option **Bearbeiten** aus.

Der Assistent Generator für Server-Tasks wird geöffnet.

2 Legen Sie auf der Seite Beschreibung den **Planungsstatus** auf **Deaktiviert** fest, und klicken Sie dann auf **Speichern**.

Aktivieren der Ordnerfreigabe für UNC- und HTTP-Repositories

Bei einem verteilten HTTP- oder UNC-Repository müssen Sie den Ordner für die Freigabe im Netzwerk aktivieren, damit der McAfee ePO-Server Dateien in das Repository kopieren kann.

Dies dient nur zu Replizierungszwecken. Verwaltete Systeme, die zum Verwenden des verteilten Repositorys konfiguriert sind, nutzen das entsprechende Protokoll (HTTP, FTP oder Windows-Dateifreigabe) und benötigen keine Ordnerfreigabe.

Vorgehensweise

1 Suchen Sie in Windows Explorer den erstellten Ordner auf dem verwalteten System.

2 Klicken Sie mit der rechten Maustaste auf den Ordner, wählen Sie Eigenschaften und dann die Registerkarte **Freigabe** aus.

3 Wählen Sie auf der Registerkarte **Freigabe** die Option **Ordner freigeben** aus.

4 Konfigurieren Sie die Freigabeberechtigungen nach Bedarf.

Systeme, die über das Repository aktualisiert werden, benötigen nur Lesezugriff, Administratorkonten hingegen (wie das Konto, das vom McAfee ePO-Server-Dienst verwendet wird) benötigen Schreibzugriff. Informationen zum Konfigurieren der entsprechenden Sicherheitseinstellungen für freigegebene Ordner finden Sie in der Microsoft Windows-Dokumentation.

5 Klicken Sie auf **OK**.

Bearbeiten von verteilten Repositories

Bearbeiten Sie nach Bedarf die Konfigurations-, Authentifizierungs- und Paketauswahloptionen eines verteilten Repositorys.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Software** | **Verteilte Repositories** und anschließend auf ein Repository.

Der Generator für verteilte Repositories wird mit den Details zum verteilten Repository geöffnet.

2 Ändern Sie die Konfigurations-, Authentifizierungs- und Paketauswahloptionen nach Bedarf.

3 Klicken Sie auf **Speichern**.

Löschen von verteilten Repositories

Sie können verteilte Repositories aus HTTP- und FTP-Servern oder UNC-Freigaben löschen. Bei diesem Vorgang werden auch die in den Repositories gespeicherten Inhalte gelöscht.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Software** | **Verteilte Repositories** und anschließend auf **Löschen** neben einem Repository.

2 Klicken Sie im Dialogfeld Repository löschen auf **OK**.

Beim Löschen des Repositorys werden die Pakete, die sich auf dem System mit dem Repository befinden, nicht gelöscht.

Gelöschte Repositories werden aus der Repository-Liste entfernt.

Verwenden von UNC-Freigaben als verteilte Repositories

Orientieren Sie sich an diesen Richtlinien, wenn Sie UNC-Freigaben als verteilte Repositories verwenden.

Bei UNC-Freigaben wird das SMB-Protokoll (Server Message Block) zum Erstellen eines freigegebenen Laufwerks verwendet. Erstellen Sie einen Benutzernamen und ein Kennwort für den Zugriff auf diese Freigabe.

Richtiges Konfigurieren der Freigabe

Stellen Sie sicher, dass die UNC-Freigabe richtig konfiguriert ist.

- **Verwenden Sie eine alternative Methode zum Schreiben in das Repository**: Melden Sie sich mit anderen Methoden beim Server an (andere Freigabe, RDP, lokal), um Daten in das Repository zu schreiben. Mischen Sie nicht das Repository, aus dem Sie lesen, und das Repository, in das Sie schreiben. Anmeldeinformationen mit Leseberechtigungen werden für Endpunkte freigegeben, und Anmeldeinformationen mit Schreibberechtigungen werden ausschließlich vom McAfee ePO-Server zum Aktualisieren des Inhalts Ihres verteilten Repositories verwendet.
- **Verwenden Sie keine Freigabe auf dem Domänen-Controller**: Erstellen Sie eine Freigabe, die sich nicht auf dem Domänen-Controller befindet. Ein lokaler Benutzer auf einem Domänen-Controller ist ein Domänenbenutzer.

Schützen des Kontos, das Sie zum Lesen von Daten aus der UNC-Freigabe verwenden

Orientieren Sie sich an diesen Richtlinien, um die Sicherheit des für den Zugriff auf die UNC-Freigabe verwendeten Kontos sicherzustellen.

- **Erteilen Sie dem Konto für die UNC-Freigabe nur Leserechte für alle mit Ausnahme des McAfee ePO-Server-Master-Repositories**: Stellen Sie beim Einrichten der Freigabe sicher, dass das erstellte Konto nur über Leserechte für das Verzeichnis und die Freigabeberechtigungen verfügt. Erteilen Sie keine Remote-Schreibrechte für die Freigabe (auch nicht für Administratoren oder andere Konten). Das gerade von Ihnen erstellte Konto sollte als einziges Konto zulässig sein.

  Über das McAfee ePO-Server-Master-Repository müssen Dateien in das UNC-Freigabekonto geschrieben werden können.

- **Erstellen Sie das Konto lokal**: Erstellen Sie das Konto in der Dateifreigabe, nicht in der Domäne. Über lokal erstellte Konten werden keine Rechte für Systeme in der Domäne erteilt.
- **Verwenden Sie ein spezielles Konto**: Erstellen Sie ein Konto speziell für das Freigeben von Repository-Daten. Verwenden Sie dieses Konto nicht für mehrere Zwecke.
- **Erteilen Sie dem Konto niedrige Berechtigungen**: Fügen Sie das Konto nicht zu Gruppen hinzu, wenn dies nicht notwendig ist. Dies gilt auch für die Gruppen "Administratoren" und "Benutzer".

- **Deaktivieren Sie überflüssige Berechtigungen**: Mit diesem Konto muss keine Anmeldung bei einem Server möglich sein. Das Konto ist ein Platzhalter, der den Zugriff auf die Dateien ermöglicht. Untersuchen Sie die Berechtigungen des Kontos, und deaktivieren Sie unnötige Berechtigungen.
- **Verwenden Sie ein sicheres Kennwort**: Verwenden Sie ein Kennwort mit 8–12 Zeichen und mehreren Zeichenattributen (Klein- und Großbuchstaben, Symbole und Zahlen). Es wird empfohlen, einen Zufallsgenerator für Kennwörter zu verwenden, damit Sie ein komplexes Kennwort erhalten.

Schützen und Warten der UNC-Freigabe

- **Schützen Sie die Freigabe mit einer Firewall**: Blockieren Sie immer nicht erforderlichen Datenverkehr. Es wird empfohlen, aus- und eingehenden Datenverkehr zu blockieren. Sie können eine Software-Firewall auf dem Server oder eine Hardware-Firewall im Netzwerk verwenden.
- **Aktivieren Sie Datei-Audits**: Aktivieren Sie immer Audit-Protokolle für Sicherheitsaspekte, um Zugriffe auf die Netzwerkfreigaben zu verfolgen. Aus diesen Protokollen geht hervor, wer auf die Freigabe zugegriffen hat, wann dies geschehen ist und welche Aktionen der Benutzer ausgeführt hat.
- **Ändern Sie die Kennwörter**: Ändern Sie die Kennwörter häufig. Achten Sie darauf, dass das neue Kennwort sicher ist, und denken Sie daran, die McAfee ePO-Konfiguration mit dem neuen Kennwort zu aktualisieren.
- **Deaktivieren Sie das Konto und die Freigabe, wenn Sie sie nicht mehr benötigen**: Wenn Sie nicht von UNC, sondern von einem anderen Repository-Typ wechseln, denken Sie daran, das Konto zu deaktivieren oder zu löschen und die Freigabe zu schließen und zu entfernen.

Verwenden von lokalen verteilten Repositories, die nicht verwaltet werden

Sie können Inhalte aus dem Master-Repository in ein verteiltes Repository kopieren, das nicht verwaltet wird.

Wenn ein nicht verwaltetes Repository erstellt wurde, müssen Sie verwaltete Systeme manuell so konfigurieren, dass sie Dateien aus dem nicht verwalteten Repository beziehen.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Kopieren Sie alle Dateien und Unterverzeichnisse im Ordner des Master-Repositories auf dem Server.

   Falls Sie zum Beispiel Windows 2008 R2 Server verwenden, ist dies der Standardpfad auf ihrem Server: `C:\Programme (x86)\McAfee\ePolicy Orchestrator\DB\Software`

2. Fügen Sie die kopierten Dateien und Unterordner in den Repository-Ordner auf dem System des verteilten Repositorys ein.

3 Konfigurieren Sie eine Agenten-Richtlinie für verwaltete Systeme zum Verwenden des neuen, nicht verwalteten verteilten Repositories:

   a Klicken Sie auf **Menü** | **Richtlinie** | **Richtlinienkatalog**, und wählen Sie dann in der Dropdown-Liste **Produkt** den Eintrag **McAfee Agent** und in der Dropdown-Liste **Kategorie** den Eintrag **Repository** aus.

   b Klicken Sie auf eine vorhandene Agenten-Richtlinie, oder erstellen Sie eine neue.

   > Auf den Registerkarten mit den Optionen für eine Richtlinie können Sie nicht festlegen, dass die Richtlinienvererbung unterbrochen werden soll. Daher müssen Sie sich beim Anwenden dieser Richtlinie vergewissern, dass nur die richtigen Systeme die Richtlinie zum Verwenden des nicht verwalteten verteilten Repositorys erhalten und erben.

   c Klicken Sie auf der Registerkarte **Repositories** auf **Hinzufügen**.

   d Geben Sie einen Namen in das Textfeld **Repository-Name** ein.

   Bei dem Namen muss es sich nicht um den Namen des Systems handeln, das als Host für das Repository dient.

   e Wählen Sie unter **Dateien abrufen von** den Typ des Repositorys aus.

   f Geben Sie unter **Konfiguration** den Speicherort des Repositorys mithilfe der entsprechenden Syntax für den Repository-Typ ein.

   g Geben Sie eine Portnummer ein, oder behalten Sie den Standardport bei.

   h Konfigurieren Sie die Anmeldeinformationen zur Authentifizierung nach Bedarf.

   i Klicken Sie auf **OK**, um das neue verteilte Repository zur Liste hinzuzufügen.

   j Wählen Sie das neue Repository in der Liste aus.

   Der Typ **Lokal** gibt an, dass es nicht von ePolicy Orchestrator verwaltet wird. Wenn in der **Repository-Liste** ein nicht verwaltetes Repository ausgewählt wird, sind die Schaltflächen **Bearbeiten** und **Löschen** aktiviert.

   k Klicken Sie auf **Speichern**.

Jedes System, auf das diese Richtlinie angewendet wird, empfängt die neue Richtlinie bei der nächsten Agent-zu-Server-Kommunikation.

Arbeiten mit den Repository-Listen-Dateien

Sie können die Repository-Listendateien exportieren.

- `SiteList.xml`: Wird vom Agenten und von unterstützten Produkten verwendet.
- `SiteMgr.xml`: Wird bei einer erneuten Installation des McAfee ePO-Servers oder beim Import auf anderen McAfee ePO-Servern verwendet, auf denen die gleichen verteilten Repositories oder Quellsites verwendet werden.

Aufgaben

- *Exportieren der Repository-Listen-Datei SITELIST.XML* auf Seite 87
  Sie können die Repository-Listen-Datei (`SITELIST.XML`) für die manuelle Ausbringung auf Systemen oder für den Import während der Installation von unterstützten Produkten exportieren.
- *Exportieren der Repository-Liste zur Sicherung oder für die Verwendung auf anderen Servern* auf Seite 87
  Mithilfe der exportierten Datei `SiteMgr.xml` können Sie verteilte Repositories und Quellsites wiederherstellen, wenn Sie den McAfee ePO-Server erneut installieren oder verteilte Repositories oder Quellsites für einen anderen McAfee ePO-Server freigeben möchten.
- *Importieren verteilter Repositories aus der Repository-Liste* auf Seite 88
  Sie importieren verteilte Repositories aus der Datei `SiteMgr.xml`, nachdem Sie einen Server neu installiert haben oder wenn auf einem Server die gleichen verteilten Repositories wie auf einem anderen Server verwendet werden sollen.
- *Importieren von Quellsites aus der Datei SITEMGR.XML* auf Seite 88
  Einen Import von Quellsites aus einer Repository-Listen-Datei führen Sie durch, nachdem Sie einen Server neu installiert haben oder wenn Sie möchten, dass zwei Server die gleichen verteilten Repositories verwenden sollen.

Exportieren der Repository-Listen-Datei SITELIST.XML

Sie können die Repository-Listen-Datei (`SITELIST.XML`) für die manuelle Ausbringung auf Systemen oder für den Import während der Installation von unterstützten Produkten exportieren.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Software** | **Master-Repository**, und klicken Sie dann auf **Aktionen** | **Sitelist exportieren**.

Das Dialogfeld Dateidownload wird angezeigt.

2 Klicken Sie auf **Speichern**, wechseln Sie zu dem Speicherort, in dem die Datei `SITELIST.XML` gespeichert werden soll, und klicken Sie dann auf **Speichern**.

Sobald Sie diese Datei exportiert haben, können Sie sie während der Installation von unterstützten Produkten importieren. Anweisungen hierzu finden Sie im *Installationshandbuch* für das entsprechende Produkt.

Sie können die Repository-Liste auch auf verwaltete Systeme verteilen und sie anschließend auf den Agenten anwenden.

Exportieren der Repository-Liste zur Sicherung oder für die Verwendung auf anderen Servern

Mithilfe der exportierten Datei `SiteMgr.xml` können Sie verteilte Repositories und Quellsites wiederherstellen, wenn Sie den McAfee ePO-Server erneut installieren oder verteilte Repositories oder Quellsites für einen anderen McAfee ePO-Server freigeben möchten.
Sie können diese Datei auf den Seiten **Verteilte Repositories** oder **Quellsites** exportieren. Wenn Sie jedoch diese Datei auf einer der beiden Seiten importieren, werden nur diejenigen Elemente aus der Datei importiert, die auf dieser Seite aufgeführt sind. Wenn zum Beispiel diese Datei auf der Seite **Verteilte Repositories** importiert wird, werden nur die verteilten Repositories in der Datei importiert. Wenn Sie also sowohl die verteilten Repositories als auch die Quellsites importieren möchten, müssen Sie die Datei jeweils von der entsprechenden Seite importieren.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Software** | **Verteilte Repositories** (oder **Quellsites**), klicken Sie dann auf **Aktionen** | **Repositories exportieren** (oder **Quellsites exportieren**).

Das Dialogfeld Dateidownload wird angezeigt.

2 Klicken Sie auf **Speichern**, wechseln Sie zu dem Speicherort, in dem die Datei gespeichert werden soll, und klicken Sie dann auf **Speichern**.

Importieren verteilter Repositories aus der Repository-Liste

Sie importieren verteilte Repositories aus der Datei `SiteMgr.xml`, nachdem Sie einen Server neu installiert haben oder wenn auf einem Server die gleichen verteilten Repositories wie auf einem anderen Server verwendet werden sollen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Software** | **Verteilte Repositories** und anschließend auf **Aktionen** | **Repositories importieren**.

Die Seite Repositories importieren wird angezeigt.

2 Wechseln Sie zur exportierten Datei `SITEMGR.XML`, wählen Sie sie aus, und klicken Sie auf **OK**. Das verteilte Repository wird in den Server importiert.

3 Klicken Sie auf **OK**.

Die ausgewählten Repositories werden zur Liste der Repositories auf diesem Server hinzugefügt.

Importieren von Quellsites aus der Datei SITEMGR.XML

Einen Import von Quellsites aus einer Repository-Listen-Datei führen Sie durch, nachdem Sie einen Server neu installiert haben oder wenn Sie möchten, dass zwei Server die gleichen verteilten Repositories verwenden sollen.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste **Einstellungskategorien** den Eintrag **Quellsites** aus, und klicken Sie dann auf **Bearbeiten**.

2 Klicken Sie auf **Importieren**.

3 Wechseln Sie zur exportierten Datei `SiteMgr.xml`, wählen Sie sie aus, und klicken Sie auf **OK**.

4 Wählen Sie die Quellsites aus, die auf diesen Server importiert werden sollen, und klicken Sie auf **OK**.

Die ausgewählten Quellsites werden zur Liste der Repositories auf diesem Server hinzugefügt.

Abruf-Tasks

Mit Abruf-Tasks können Sie das Master-Repository mit den Aktualisierungspaketen für DAT-Dateien und Scan-Module aus der Quellsite aktualisieren.

DAT- und Scan-Modul-Dateien müssen häufig aktualisiert werden. McAfee veröffentlicht neue DAT-Dateien täglich und Scan-Modul-Dateien etwas seltener. Bringen Sie diese Pakete so schnell wie möglich auf die verwalteten Systemen aus, um diese vor den neuesten Bedrohungen zu schützen.

Sie können angeben, welche Pakete aus der Quellsite in das Master-Repository kopiert werden sollen.

EXTRA.DAT-Dateien müssen manuell in das Master-Repository eingecheckt werden. Diese Dateien stehen auf der McAfee-Website zur Verfügung.

Ein geplanter Server-Task für Repository-Abrufe wird automatisch und regelmäßig zu den von Ihnen festgelegten Zeiten ausgeführt. So können Sie beispielsweise einen wöchentlichen Repository-Abruf-Task für jeden Donnerstag um 05:00 Uhr planen.

Sie können den Task Jetzt abrufen auch so planen, dass Aktualisierungen sofort in das Master-Repository eingecheckt werden, zum Beispiel wenn McAfee Sie vor einem sich schnell ausbreitenden Virus warnt und zum Schutz vor diesen Virus eine neue DAT-Datei veröffentlicht.

Wenn ein Abruf-Task fehlschlägt, müssen Sie die Pakete manuell in das Master-Repository einchecken.

Nach dem Aktualisieren des Master-Repositorys können Sie diese Aktualisierungen mit Replizierungs-Tasks oder über die globale Aktualisierung automatisch in Ihren Systemen verteilen.

Erwägungen beim Planen von Abruf-Tasks

Berücksichtigen Sie beim Planen von Abruf-Tasks Folgendes:

- **Auslastung von Bandbreite und Netzwerk** – Wenn Sie (wie empfohlen) die globale Aktualisierung verwenden, sollten Sie die Ausführung von Abruf-Tasks für Zeiten planen, zu denen das Netzwerk nicht so sehr von anderen Ressourcen in Anspruch genommen wird. Bei der globalen Aktualisierung werden die Aktualisierungsdateien automatisch verteilt, sobald der Abruf-Task abgeschlossen ist.
- **Häufigkeit des Tasks** – DAT-Dateien werden täglich veröffentlicht, was Sie aber möglicherweise nicht täglich in Anspruch nehmen möchten.
- **Replizierungs- und Aktualisierungs-Tasks** – Planen Sie Replizierungs- und Client-Aktualisierungs-Tasks, um sicherzustellen, dass alle Aktualisierungsdateien in Ihrer Umgebung verteilt werden.

Replizierungs-Tasks

Verwenden Sie Replizierungs-Tasks zum Kopieren von Inhalten des Master-Repositorys in verteilte Repositories. Replizieren Sie Inhalte im Master-Repository in alle verteilten Repositories. Andernfalls können diese Aktualisierungen von einigen Systemen nicht empfangen werden. Stellen Sie sicher, dass alle verteilten Repositories aktuell sind.

Wenn Sie alle Aktualisierungen global vornehmen, sind Replizierungs-Tasks für Ihre Umgebung unter Umständen nicht erforderlich. Allerdings werden sie zur Absicherung empfohlen. Wenn Sie Aktualisierungen dagegen generell nicht global vornehmen, müssen Sie einen Server-Task vom Typ "Repository-Replizierung" planen oder einen Task vom Typ "Jetzt replizieren" ausführen.

Um zu gewährleisten, dass die verteilten Repositories auf dem neuesten Stand sind, sollten Sie regelmäßige Server-Tasks zur Repository-Replizierung planen. Mit dem Planen von täglichen Replizierungs-Tasks stellen Sie sicher, dass die verwalteten Systeme aktuell bleiben. Automatisieren Sie die Replizierung in Ihre verteilten Repositories, indem Sie Repository-Replizierungs-Tasks verwenden.

Gelegentlich müssen Sie an Ihrem Master-Repository Änderungen vornehmen, die Sie sofort in Ihren verteilten Repositories replizieren möchten, statt auf die nächste geplante Replizierung zu warten. Führen Sie in diesem Fall einen Task "Jetzt replizieren" aus, um Ihre verteilten Repositories manuell zu aktualisieren.

Vergleich von vollständiger und inkrementeller Replizierung

Wählen Sie beim Erstellen eines Replizierungs-Tasks für die Replizierung **Inkrementell** oder **Vollständig** aus. Bei inkrementeller Replizierung werden nur die neuen Aktualisierungen im Master-Repository kopiert, die sich noch nicht im verteilten Repository befinden. Dadurch sinkt die Netzwerkbelastung. Bei einer vollständigen Replizierung wird der gesamte Inhalt des Master-Repositorys kopiert.

Es wird empfohlen, einen täglichen inkrementellen Replizierungs-Task zu planen. Wenn Dateien im verteilten Repository außerhalb der ePolicy Orchestrator-eigenen Replizierungsfunktion gelöscht werden können, planen Sie einen wöchentlichen Task für eine vollständige Replizierung.

Repository-Auswahl

Neue verteilte Repositories werden zur Repository-Listen-Datei hinzugefügt, die alle verfügbaren verteilten Repositories enthält. Die Agenten der verwalteten Systeme aktualisieren diese Datei bei jeder Kommunikation mit dem McAfee ePO-Server. Bei jedem Start des Agenten-Dienstes (**McAfee Framework-Dienst**) und bei Änderungen der Repository-Liste wird ein Repository vom Agenten ausgewählt.

Durch die selektive Replizierung kann die Aktualisierung einzelner Repositories besser gesteuert werden. Wenn Sie Replizierungs-Tasks planen, haben Sie folgende Möglichkeiten:

- Wählen Sie bestimmte verteilte Repositories, auf die der Task angewendet werden soll. Durch das Replizieren auf verschiedene verteilte Repositories zu unterschiedlichen Uhrzeiten wird die erforderliche Bandbreite reduziert. Diese Repositories können beim Erstellen oder Bearbeiten des Replizierungs-Tasks angegeben werden.
- Wählen Sie bestimmte Dateien und Signaturen, die auf verteilte Repositories repliziert werden sollen. Wenn Sie auswählen, welche Dateitypen für jedes System erforderlich sind, das sich in das verteilte Repository eincheckt, wird die erforderliche Bandbreite reduziert. Wenn Sie Ihre verteilten Repositories definieren oder bearbeiten, können Sie festlegen, welche Pakete in das verteilte Repository repliziert werden sollen.

Diese Funktion ist für das Aktualisieren von Produkten gedacht, die nur auf einem Teil der Systeme in Ihrer Umgebung installiert sind, z. B. VirusScan Enterprise. Mithilfe der Funktion können Sie diese Aktualisierungen auf die verteilten Repositories beschränken, die diese Systeme verwenden.

Auswählen von Repositories durch Agenten

Standardmäßig können Agenten versuchen, Aktualisierungen von jedem Repository in der Repository-Listen-Datei durchzuführen. Agenten können mithilfe einer Netzwerk-ICMP-Ping-Abfrage oder einem Subnetzadressen-Vergleichsalgorithmus das verteilte Repository mit der kürzesten Reaktionszeit suchen. Meist ist dies das verteilte Repository, das sich im Netzwerk dem System am nächsten befindet.

Wenn Sie verteilte Repositories in der Agenten-Richtlinie aktivieren oder deaktivieren, können Sie steuern, welche verteilten Repositories die Agenten zum Aktualisieren verwenden. Sie sollten Repositories in den Richtlinieneinstellungen jedoch nicht deaktivieren. Wenn die Agenten sich über ein beliebiges verteiltes Repository aktualisieren können, wird gewährleistet, dass sie die Aktualisierungen erhalten.

7 Registrierte Server

Sie können auf zusätzliche Server zugreifen, indem Sie sie bei Ihrem McAfee ePO-Server registrieren. Mithilfe registrierter Server können Sie Ihre Software auf externen Servern integrieren. Beispielsweise können Sie einen LDAP-Server für die Verbindung mit Ihrem Active Directory-Server registrieren.

In McAfee ePO ist die Kommunikation mit folgenden Servern möglich:

- Andere McAfee ePO-Server
- Zusätzlichen Remote-Datenbank-Servern
- LDAP-Servern
- Syslog-Server

Damit Sie diesen registrierten Server konfigurieren können, müssen McAfee Endpoint Security und die Erweiterung für die Syslog-Verwaltung in Ihrer McAfee ePO-Umgebung installiert sein.

Jeder dieser Typen von registrierten Servern unterstützt oder ergänzt die Funktion von ePolicy Orchestrator und anderen Erweiterungen und Produkten von McAfee und von Drittanbietern.

Inhalt

- *Registrieren von McAfee ePO-Servern*
- *Registrieren von LDAP-Servern*
- *Registrieren von SNMP-Servern*
- *Verwenden von Datenbank-Servern*
- *Freigeben von Objekten zwischen Servern*

Registrieren von McAfee ePO-Servern

Sie können zusätzliche McAfee ePO-Server registrieren, um sie zusammen mit dem McAfee ePO-Haupt-Server zum Erfassen oder Aggregieren von Daten zu verwenden oder verwaltete Systeme zwischen den registrierten Servern übertragen zu können.

Bevor Sie beginnen

Zum Registrieren eines McAfee ePO-Servers bei einem anderen benötigen Sie detaillierte Informationen zur SQL-Datenbank des McAfee ePO-Servers, den Sie registrieren möchten. Mit dem folgenden Remote-Befehl können Sie unter anderem den Namen des Microsoft SQL-Datenbank-Servers und der Datenbank ermitteln:

```
https://<Server-Name>:<Port>/core/config
```

Die folgenden Variablen werden im Remote-Befehl verwendet:

- `<Server-Name>`: Dies ist der DNS-Server-Name oder die IP-Adresse des McAfee ePO-Remote-Servers.
- `<Port>`: Dies ist die zugewiesene McAfee ePO-Server-Portnummer, in der Regel "`8443`", sofern Sie für den Server keine andere Portnummer konfiguriert haben.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie **Menü** | **Konfiguration** | **Registrierte Server** aus, und klicken Sie dann auf **Neuer Server**.

2 Wählen Sie auf der Seite Beschreibung im Menü Server-Typ die Option **ePO** aus, geben Sie einen eindeutigen Namen sowie Anmerkungen ein, und klicken Sie dann auf **Weiter**.

3 Geben Sie zum Konfigurieren des Servers die folgenden Informationen an:

Option	Definition
Authentifizierungstyp	Gibt an, welcher Typ von Authentifizierung für diese Datenbank verwendet werden soll. Dazu gehören: • **Windows-Authentifizierung** • **SQL-Authentifizierung**
Client-Task-Freigabe	Gibt an, ob der Client-Task für diesen Server aktiviert oder deaktiviert sein soll.
Datenbankname	Geben Sie den Namen für diese Datenbank an.
Datenbankport	Geben Sie den Port für diese Datenbank an.
Datenbank-Server	Geben Sie den Namen der Datenbank für diesen Server an. Sie können eine Datenbank mithilfe des DNS-Namens oder der IP-Adresse (IPv4 oder IPv6) angeben.
ePO-Version	Gibt die Version des McAfee ePO-Servers an, der registriert werden soll.
Kennwort	Geben Sie das Kennwort für diesen Server an.
Richtlinienfreigabe	Gibt an, ob die Richtlinienfreigabe für diesen Server aktiviert oder deaktiviert sein soll.
SQL-Server-Instanz	Hier können Sie festlegen, ob es sich um den standardmäßigen Server oder eine bestimmte Instanz handelt. Geben Sie für eine bestimmte Instanz den Instanznamen an. Bevor Sie eine Verbindung zu einer bestimmten SQL-Instanz mit deren Instanznamen herstellen, müssen Sie sicherstellen, dass der SQL Browser-Dienst ausgeführt wird. Wenn der SQL Browser-Dienst nicht ausgeführt wird, geben Sie die Portnummer an. Wählen Sie die standardmäßige SQL-Server-Instanz aus, und geben Sie die Portnummer ein, um eine Verbindung zu der SQL-Server-Instanz herzustellen.
SSL-Kommunikation mit Datenbank-Server	Gibt an, ob SSL (Secure Socket Layer) für die Kommunikation zwischen ePolicy Orchestrator und diesem Datenbank-Server verwendet wird. Die folgenden Optionen sind möglich: • **SSL verwenden (wenn möglich)** • **Immer SSL verwenden** • **Niemals SSL verwenden**

Option	Definition
Verbindung testen	Überprüft die Verbindung für den beschriebenen Server. Wenn Sie einen Server mit einer anderen McAfee ePO-Version registrieren, wird die folgende rein informative Warnung angezeigt: Warnung: Versionen stimmen nicht überein.
Systeme übertragen	Gibt an, ob die Fähigkeit zum Übertragen von Systemen bei diesem Server aktiviert oder deaktiviert ist. Wenn diese Option aktiviert ist, wählen Sie **Automatischer Sitelist-Import** oder **Manueller Sitelist-Import** aus. Bei Auswahl von **Manueller Sitelist-Import** besteht die Möglichkeit, dass in älteren Versionen von McAfee Agent (Version 4.0 und niedriger) kein Kontakt mehr zum Agenten-Handler aufgenommen werden kann. Dies ist in folgenden Fällen möglich: • Sie übertragen Systeme von diesem McAfee ePO-Server auf den registrierten McAfee ePO-Server, • und der Name eines Agenten-Handlers wird alphanumerisch vor dem McAfee ePO-Server-Namen in der angegebenen Sitelist angezeigt. • die älteren Agenten diese Agentensteuerung verwenden.
NTLMv2 verwenden	Sie können optional auswählen, dass das NT-LAN-Manager-Authentifizierungsprotokoll verwendet werden soll. Wählen Sie diese Option aus, wenn das Protokoll auf dem zu registrierenden Server verwendet wird.
Benutzername	Geben Sie den Benutzernamen für diesen Server an.

4 Klicken Sie auf **Speichern**.

Registrieren von LDAP-Servern

Sie benötigen einen registrierten LDAP-Server (Lightweight Directory Access Protocol), um Richtlinienzuweisungsregeln verwenden sowie dynamisch zugewiesene Berechtigungssätze und die Active Directory-Benutzeranmeldung aktivieren zu können.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie **Menü** | **Konfiguration** | **Registrierte Server** aus, und klicken Sie dann auf **Neuer Server**.

2 Wählen Sie auf der Seite **Beschreibung** im Menü **Server-Typ** die Option **LDAP-Server** aus, geben Sie einen eindeutigen Namen und eine Beschreibung an, und klicken Sie dann auf **Weiter**.

3 Wählen Sie in der Liste **LDAP-Server-Typ** aus, ob Sie einen OpenLDAP- oder einen Active Directory-Server registrieren möchten.

Bei den nachfolgenden Anweisungen wird davon ausgegangen, dass ein Active Directory-Server konfiguriert werden soll. Wo erforderlich, sind entsprechende Informationen für OpenLDAP-Server aufgeführt.

4 Wählen Sie im Abschnitt **Server-Name** aus, ob Sie einen Domänennamen oder den Namen eines bestimmten Servers angeben möchten.

Verwenden Sie Domänennamen im DNS-Format (z. B. `interneDomäne.com`) und vollqualifizierte Domänennamen oder IP-Adressen für Server (z. B. `server1.interneDomäne.com` oder 192.168.75.101).

Bei Verwendung von Domänennamen haben Sie Failover-Unterstützung und erhalten die Möglichkeit, nur Server von einer bestimmten Site auszuwählen (wenn gewünscht).

Bei OpenLDAP-Servern können nur Server-Namen verwendet werden. Sie können nicht nach der Domäne angegeben werden.

5 Wählen Sie aus, ob Sie den **Globalen Katalog verwenden** möchten.

Diese Option ist standardmäßig deaktiviert. Eine Aktivierung kann zu deutlichen Verbesserungen bei der Leistung führen. Diese Option sollte jedoch nur dann aktiviert werden, wenn es sich bei der registrierten Domäne um die übergeordnete Domäne von nur lokalen Domänen handelt. Wenn sie auch nicht-lokale Domänen enthält, kann beim Verfolgen von Weiterleitungen beträchtlicher nicht-lokaler Netzwerkverkehr anfallen, was sich möglicherweise negativ auf die Leistung auswirkt.

Die Option **Globalen Katalog verwenden** steht bei OpenLDAP-Servern nicht zur Verfügung.

6 Wenn Sie den globalen Katalog nicht verwenden möchten, können Sie wahlweise **Weiterleitung suchen** aktivieren.

Das Suchen von Weiterleitungen kann sich negativ auf die Leistung auswirken, wenn durch diese Funktion nicht-lokaler Netzwerkverkehr verursacht wird (wobei es keine Rolle spielt, ob ein globaler Katalog verwendet wird).

7 Legen Sie mithilfe der Option **SSL verwenden** fest, ob mit diesem Server über SSL kommuniziert werden soll.

8 Wenn Sie einen OpenLDAP-Server konfigurieren, geben Sie den **Port** ein.

9 Geben Sie **Benutzername** und **Kennwort** ein.

Das sollten die Anmeldeinformationen für ein Administratorkonto auf dem Server sein. Verwenden Sie für Active Directory-Server das Format `Domäne\Benutzername`, und für OpenLDAP-Server das Format `cn=Benutzer,dc=Domäne,dc=com`.

10 Geben Sie entweder einen **Site-Namen** für den Server ein, oder wählen Sie einen Namen aus, indem Sie auf **Durchsuchen** klicken und zu der Site wechseln.

11 Klicken Sie auf **Verbindung testen**, um zu überprüfen, ob die Kommunikation mit dem Server wie angegeben funktioniert. Falls erforderlich, ändern Sie die Informationen.

12 Klicken Sie auf **Speichern**, um den Server zu registrieren.

Registrieren von SNMP-Servern

Zum Empfangen eines SNMP-Traps müssen Sie die SNMP-Server-Informationen hinzufügen, damit ePolicy Orchestrator weiß, wohin der Trap gesendet werden soll.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Konfiguration** | **Registrierte Server**, und klicken Sie dann auf **Neuer Server**.

2 Wählen Sie auf der Seite **Beschreibung** als Server-Typ den Eintrag **SNMP-Server** aus, geben Sie den Namen und mögliche weitere Informationen zu dem Server an, und klicken Sie dann auf **Weiter**.

3 Wählen Sie in der Dropdown-Liste **URL-Adresse** einen der folgenden Typen für Server-Adressen aus, und geben Sie dann die Adresse ein:

- **DNS-Name** – Gibt den DNS-Namen des registrierten Servers an.
- **IPv4** – Gibt die IPv4-Adresse des registrierten Servers an.
- **IPv6** – Gibt den DNS-Namen des registrierten Servers an, der eine IPv6-Adresse hat.

4 Wählen Sie die von Ihrem Server verwendete SNMP-Version aus:

- Wenn Sie als SNMP-Server-Version **SNMPv1** oder **SNMPv2c** auswählen, geben Sie unter **Sicherheit** die Community-Zeichenfolge des Servers ein.
- Wenn Sie **SNMPv3** auswählen, geben Sie die Details für die **SNMPv3-Sicherheit** an.

5 Klicken Sie auf **Test-Trap senden**, um Ihre Konfiguration zu testen.

6 Klicken Sie auf **Speichern**.

Der hinzugefügte SNMP-Server wird auf der Seite Registrierte Server angezeigt.

Verwenden von Datenbank-Servern

ePolicy Orchestrator kann Daten nicht nur von eigenen Datenbanken abrufen, sondern auch von Erweiterungsdatenbanken.

Zum Durchführen von Tasks in ePolicy Orchestrator müssen Sie möglicherweise eine Reihe unterschiedlicher Server-Typen registrieren. Dazu können Authentifizierungsserver, Active Directory-Kataloge, McAfee ePO-Server und Datenbankserver gehören, die mit bestimmten von Ihnen installierten Erweiterungen zusammenarbeiten.

Datenbanktypen

Mit einer Erweiterung kann ein *Datenbanktyp* (der auch als "Schema" oder "Struktur" bezeichnet wird) bei ePolicy Orchestrator registriert werden. Anschließend kann diese Erweiterung Daten für Abfragen, Berichte, Dashboard-Monitore und Server-Tasks bereitstellen. Um diese Daten zu verwenden, müssen Sie den Server zunächst bei ePolicy Orchestrator registrieren.

Datenbank-Server

Ein *Datenbankserver* ist eine Kombination aus einem Server und einem auf diesem Server installierten Datenbanktyp. Ein Server kann als Host für mehr als eine Datenbank dienen, und ein Datenbanktyp kann auf mehreren Servern installiert sein. Jede Kombination der beiden Komponenten muss separat registriert werden und wird als *Datenbankserver* bezeichnet.

Nachdem Sie einen Datenbank-Server registriert haben, können Sie in Abfragen, Berichten, Dashboard-Monitoren und Server-Tasks Daten aus der Datenbank abrufen. Wenn mehrere Datenbanken mit dem gleichen Datenbanktyp registriert sind, müssen Sie eine der Datenbanken als Standardeinstellung für diesen Datenbanktyp auswählen.

Registrieren eines Datenbank-Servers

Bevor Sie Daten von einem Datenbank-Server abrufen können, müssen Sie diesen bei ePolicy Orchestrator registrieren.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Öffnen Sie die Seite **Registrierte Server**. Wählen Sie **Menü** | **Konfiguration** | **Registrierte Server** aus, und klicken Sie dann auf **Neuer Server**.
2. Wählen Sie in der Dropdown-Liste **Server-Typ** den Eintrag **Datenbank-Server** aus, geben Sie einen Server-Namen und optional eine Beschreibung ein, und klicken Sie dann auf **Weiter**.
3. Wählen Sie in der Dropdown-Liste der registrierten Typen einen **Datenbanktyp** aus. Geben Sie an, ob dieser Datenbanktyp als Standardeinstellung dienen soll.

   Wenn diesem Datenbanktyp bereits eine Standarddatenbank zugewiesen wurde, ist diese in der Zeile **Aktuelle Standarddatenbank für Datenbanktyp** angegeben.
4. Geben Sie den **Datenbankhersteller** an. Derzeit werden nur Microsoft SQL Server und MySQL unterstützt.
5. Geben Sie die Verbindungs- und Anmeldeinformationen für den Datenbank-Server ein.
6. Wenn Sie überprüfen möchten, ob alle Verbindungs- und Anmeldeinformationen korrekt eingegeben sind, klicken Sie auf **Verbindung testen**.

   Eine Statusmeldung zeigt an, ob der Vorgang erfolgreich war oder nicht.
7. Klicken Sie auf **Speichern**.

Ändern einer Datenbankregistrierung

Wenn Verbindungs- oder Anmeldeinformationen für einen Datenbank-Server geändert werden, müssen Sie die Registrierung entsprechend anpassen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Öffnen Sie die Seite **Registrierte Server**, indem Sie **Menü** | **Konfiguration** | **Registrierte Server** auswählen.
2. Wählen Sie die zu bearbeitende Datenbank aus, und klicken Sie dann auf **Aktionen** | **Bearbeiten**.
3. Ändern Sie den Namen oder die Anmerkungen für den Server, und klicken Sie dann auf **Weiter**.
4. Ändern Sie die Informationen entsprechend. Wenn Sie die Datenbankverbindung überprüfen müssen, klicken Sie auf **Verbindung testen**.
5. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Entfernen einer registrierten Datenbank

Wenn Datenbanken nicht mehr benötigt werden, können Sie sie aus dem System entfernen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Öffnen Sie die Seite **Registrierte Server**. Wählen Sie dazu **Menü** | **Konfiguration** | **Registrierte Server** aus.
2. Wählen Sie die zu löschende Datenbank aus, und klicken Sie auf **Aktionen** | **Löschen**.
3. Klicken Sie im angezeigten Bestätigungsdialogfeld auf **Ja**, um die Datenbank zu löschen.

Die Datenbank wurde gelöscht. Abfragen, Berichte oder andere Elemente in ePolicy Orchestrator, die die gelöschte Datenbank verwendet haben, werden als ungültig gekennzeichnet, bis sie einer anderen Datenbank zugeordnet werden.

Freigeben von Objekten zwischen Servern

Oftmals können Sie bestimmte Verhaltensweise eines McAfee ePO-Servers am einfachsten auf einem anderen Server replizieren, indem Sie das Element, das dieses Verhalten beschreibt, exportieren und auf dem anderen Server importieren.

Exportieren von Objekten und Daten aus dem McAfee ePO-Server

Exportierte Objekte und Daten können verwendet werden, um wichtige Daten zu sichern und die McAfee ePO-Server in einer Umgebung wiederherzustellen oder zu konfigurieren.

Die meisten in einem Server verwendeten Daten und Objekte können exportiert oder heruntergeladen werden, um angezeigt, umgewandelt oder in andere Server oder Anwendungen importiert zu werden. In der folgenden Tabelle finden Sie die verschiedenen Elemente, für die Sie Aktionen ausführen können. Zum Anzeigen von Daten exportieren Sie die Tabellen als HTML- oder PDF-Dateien. Zum Verwenden der Daten in anderen Anwendungen exportieren Sie die Tabellen als CSV- oder XML-Dateien.

Vorgehensweise

1. Klicken Sie auf der Seite, auf der die Objekte oder Daten angezeigt werden, auf **Aktionen**, und wählen Sie eine Option aus. So wählen Sie zum Beispiel beim Exportieren einer Tabelle die Option **Tabelle exportieren** aus und klicken dann auf **Weiter**.
2. Beim Exportieren von Inhalten, die in mehreren Formaten heruntergeladen werden können (beispielsweise Abfragedaten), wird die Seite **Exportieren** mit Konfigurationsoptionen angezeigt. Geben Sie die gewünschten Einstellungen an, und klicken Sie dann auf **Exportieren**.
3. Beim Exportieren von Objekten oder Definitionen (beispielsweise Client-Task-Objekte oder Definitionen) tritt eines der folgenden Ereignisse auf:
   - Es wird ein Browser-Fenster geöffnet, in dem Sie **Öffnen** oder **Speichern** auswählen können.
   - Die Seite **Exportieren** wird mit einem Link zu der Datei geöffnet. Klicken Sie mit der linken Maustaste auf den Link, um die Datei im Browser anzuzeigen, oder klicken Sie mit der rechten Maustaste auf den Link, um die Datei zu speichern.

Importieren von Elementen in ePolicy Orchestrator

Aus einem McAfee ePO-Server exportierte Elemente können in einen anderen Server importiert werden.

ePolicy Orchestrator exportiert Elemente in XML-Dateien. Diese XML-Dateien enthalten genaue Beschreibungen der exportierten Elemente.

Importieren von Elementen

Beim Importieren von Elementen in ePolicy Orchestrator müssen bestimmte Regeln beachtet werden:

- Bis auf Benutzer werden alle Elemente standardmäßig mit privater Sichtbarkeit importiert. Andere Berechtigungen können Sie während oder nach dem Import anwenden.
- Wenn ein Element mit dem gleichen Namen bereits vorhanden ist, wird dem Namen des importierten Elements die Zeichenfolge "`(importiert)`" oder "`(Kopie)`" angefügt.
- Importierte Elemente, die eine Erweiterung oder ein Produkt benötigen, die bzw. das auf dem neuen Server nicht vorhanden ist, werden als ungültig gekennzeichnet.

In ePolicy Orchestrator können nur von ePolicy Orchestrator exportierte XML-Dateien importiert werden.

Genauere Angaben dazu, wie die verschiedenen Arten von Elementen importiert werden, finden Sie in den Dokumentationen zu den einzelnen Elementen.

8 Agentensteuerungen

Agentensteuerungen leiten die Kommunikation zwischen Agenten und dem McAfee ePO-Server weiter.

Auf jedem McAfee ePO-Server befindet sich eine Master-Agentensteuerung. Sie können zusätzliche Agentensteuerungen auf Systemen im Netzwerk installieren.

Das Einrichten weiterer Agentensteuerungen bietet die folgenden Vorteile.

- Bessere Verwaltung einer größeren Anzahl von Produkten und Systemen über einen einzigen logischen McAfee ePO-Server, vorausgesetzt, die CPU auf dem Datenbank-Server wird nicht überlastet.
- Fehlertoleranz und Lastausgleich bei der Kommunikation mit vielen Agenten (einschließlich räumlich verteilter Agenten)

Inhalt

- *Funktionsweise von Agenten-Handlern*
- *Verbinden eines Agenten-Handlers in der DMZ mit einem McAfee ePO-Server in einer Domäne*
- *Steuerungsgruppen und -priorität*
- *Verwalten von Agentensteuerungen*

Funktionsweise von Agenten-Handlern

Durch Agenten-Handler wird der bei der Agent-Server-Kommunikation anfallende Netzwerkverkehr verteilt. Dabei werden verwaltete Systeme oder Gruppen von Systemen angewiesen, sich an einen bestimmten Agenten-Handler zu wenden. Nach der Zuweisung kommuniziert ein verwaltetes System anstatt mit dem McAfee ePO-Hauptserver mit dem ihm zugewiesenen Agenten-Handler.

Der Handler verfügt wie der McAfee ePO-Server über aktualisierte Sitelists, Richtlinien und Richtlinienzuweisungsregeln. Außerdem wird von ihm der Inhalt des Master-Repositories zwischengespeichert, sodass Produktaktualisierungspakete, DAT-Dateien und andere benötigte Informationen von Agenten abgerufen werden können.

Wenn der Handler beim Einchecken eines Agenten nicht über die benötigten Aktualisierungen verfügt, werden diese aus dem zugewiesenen Repository abgerufen und zwischengespeichert. Dabei wird die Aktualisierung an den Agenten weitergegeben.

Die Authentifizierung der Domänenanmeldeinformationen durch den Agenten-Handler muss möglich sein. Andernfalls muss für das Konto, über das der Agenten-Handler gegenüber der Datenbank authentifiziert wird, SQL-Authentifizierung verwendet werden. Weitere Informationen zur Windows- und SQL-Authentifizierung finden Sie in der Dokumentation für Microsoft SQL Server.

Weitere Informationen zum Ändern der Authentifizierungsmodi finden Sie in der Dokumentation für Microsoft SQL Server. Wenn Sie dies tun, müssen Sie auch die Verbindungsinformationen in SQL Server aktualisieren.

In dem Diagramm Systeme pro Agenten-Handler werden alle installierten Agenten-Handler sowie die Anzahl der von jedem Handler verwalteten Agenten angezeigt.

Deinstallierte Agenten-Handler werden in diesem Diagramm nicht angezeigt. Wenn ein Agenten-Handler deinstalliert wurde, dem von einer Zuweisungsregel für Agenten-Handler exklusiv Agenten zugewiesen sind, wird er im Diagramm als **Agenten-Handler deinstalliert** geführt und die Anzahl der Agenten angezeigt, die immer noch versuchen, eine Verbindung mit diesem Handler herzustellen.

Wenn die Agenten-Handler nicht ordnungsgemäß installiert sind, wird die Meldung **Agenten-Handler deinstalliert** angezeigt. Dies bedeutet, dass die Kommunikation zwischen dem Handler und bestimmten Agenten nicht möglich ist. Klicken Sie auf die Liste, um die Agenten anzuzeigen, bei denen keine Kommunikation mit dem Handler möglich ist.

Mehrere Agenten-Handler

Ein Netzwerk kann auch über mehrere Agenten-Handler verfügen. Angenommen Sie besitzen zahlreiche verwaltete Systeme, die über mehrere geografische Standorte oder Ländergrenzen hinweg verteilt sind. In solchen und ähnlichen Fällen können Sie ein Unternehmen zu den verwalteten Systemen hinzufügen, indem Sie verschiedene Gruppen unterschiedlichen Handlern zuweisen.

Verbinden eines Agenten-Handlers in der DMZ mit einem McAfee ePO-Server in einer Domäne

Wenn sich der McAfee ePO-Server in einer Domäne befindet, ist keine Verbindung von einem in der DMZ installierten Agenten-Handler zur McAfee ePO-SQL-Datenbank möglich, da Domänenanmeldeinformationen vom Agenten-Handler nicht verwendet werden können.

Diese Einschränkung können Sie umgehen, indem Sie den Agenten-Handler so konfigurieren, dass die Anmeldeinformationen für das Konto des SQL-Datenbank-Systemadministrators (SA) verwendet werden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Aktivieren Sie das Systemadministratorkonto.

   a Öffnen Sie **SQL Management Studio**, erweitern Sie **Sicherheit** | **Anmeldungen**, und doppelklicken Sie auf das SA-Konto.

   b Geben Sie auf der Registerkarte **Allgemein** das Kennwort ein, und bestätigen Sie es.

   c Legen Sie auf der Registerkarte **Status** die Option **Anmeldung** auf **Aktiviert** fest, und klicken Sie dann auf **OK**.

   d Klicken Sie mit der rechten Maustaste auf den Namen der Datenbankinstanz, und klicken Sie auf **Eigenschaften**.

   Das Systemadministratorkonto ist aktiviert.

2 Ändern Sie das Systemadministratorkonto, um eine Verbindung mit der McAfee ePO-Datenbank herzustellen.

   a Öffnen Sie einen Web-Browser, und wechseln Sie zu https://localhost:8443/core/config-auth.

   > 8443 ist der Konsolen-Kommunikationsport. Wenn Sie für den Zugriff auf die McAfee ePO-Konsole einen anderen Port verwenden, schließen Sie diese Portnummer in die Adresse ein.

   b Melden Sie sich mit Ihren McAfee ePO-Anmeldeinformationen an.

c Löschen Sie den Eintrag im Feld **Benutzerdomäne**, und geben Sie dann **sa** ein.

d Geben Sie ein Kennwort für das Systemadministratorkonto ein, und klicken Sie dann auf **Verbindung testen**.

e Wenn der Test erfolgreich verläuft, klicken Sie auf **Übernehmen**.

Anderenfalls geben Sie das Kennwort erneut ein, und klicken Sie dann wieder auf **Verbindung testen**.

Vom Agenten-Handler werden die Anmeldeinformationen des Systemadministrators für die Kommunikation mit der McAfee ePO-Datenbank verwendet.

Steuerungsgruppen und -priorität

Bei Verwendung mehrerer Agentensteuerungen in einem Netzwerk sollten Sie diese gruppieren und priorisieren, um Netzwerkverbindungen sicherzustellen.

Steuerungsgruppen

Bei mehreren Agentensteuerungen in einem Netzwerk können Sie Steuerungsgruppen erstellen. Außerdem können Sie den Steuerungen in einer Gruppe Prioritäten zuweisen. Anhand der Steuerungspriorität erkennen die Agenten, mit welcher Steuerung sie zuerst kommunizieren sollen. Wenn die Steuerung mit der höchsten Priorität nicht verfügbar ist, wechselt der Agent zur nächsten Steuerung in der Liste. Die Prioritätsinformationen sind in der Repository-Liste (SITELIST.XML) in jedem Agenten enthalten. Wenn Sie Steuerungszuweisungen ändern, wird diese Datei während der Agent-zu-Server-Kommunikation aktualisiert. Nach dem Empfang der Zuweisung wartet der Agent mit deren Implementierung bis zur nächsten regelmäßig geplanten Kommunikation. Wenn Sie den Agenten sofort aktualisieren möchten, können Sie eine sofortige Agenten-Reaktivierung ausführen.

Das Gruppieren von Steuerungen und Zuweisen von Prioritäten lässt sich gemäß den Anforderungen der jeweiligen Umgebung anpassen. Für das Gruppieren von Steuerungen gibt es zwei Szenarien:

- **Verwenden mehrerer Steuerungen für den Lastausgleich**

  Sie haben ein Netzwerk mit einer großen Anzahl von verwalteten Systemen, für die die aus der Agent-zu-Server-Kommunikation und der Erzwingung von Richtlinien resultierende Netzwerklast möglichst verteilt werden soll. Sie können die Steuerungsliste so konfigurieren, dass die Agenten die Steuerungen, mit denen sie kommunizieren, nach dem Zufallsprinzip auswählen.

- **Einrichten eines alternativen Plans zum Sicherstellen der Agent-zu-Server-Kommunikation**

  Sie haben Systeme, die über mehrere geographische Standorte verteilt sind. Indem Sie jeder über diese Standorte verteilten Steuerung eine Priorität zuweisen, können Sie angeben, mit welchen Steuerungen die Agenten in welcher Reihenfolge kommunizieren sollen. So kann sichergestellt werden, dass die verwalteten Systeme in einem Netzwerk auf dem aktuellen Stand bleiben, indem alternative Kommunikationsmöglichkeiten für Agenten erstellt werden (so wie mit alternativen Repositories sichergestellt wird, dass den Agenten immer neue Aktualisierungen zur Verfügung stehen). Wenn die Steuerung mit der höchsten Priorität nicht verfügbar ist, wechselt der Agent zur Steuerung mit der nächsthöheren Priorität.

Außer innerhalb einer Gruppe von Steuerungen können Sie Steuerungsprioritäten auch über mehrere Gruppen von Steuerungen hinweg zuweisen. Auf diese Weise wird Ihre Umgebung weiter abgesichert, und Sie erhöhen damit die Wahrscheinlichkeit, dass Ihre Agenten jederzeit die benötigten Informationen empfangen können.

Sitelist-Dateien

Mithilfe der Dateien SITELIST.XML und SITELIST.INFO entscheidet der Agent, mit welcher Steuerung er kommuniziert. Diese Dateien werden bei jeder Aktualisierung der Steuerungszuweisungen und -prioritäten auf dem verwalteten System aktualisiert. Nachdem die Dateien aktualisiert wurden, implementiert der Agent die neue Zuweisung oder Priorität bei der nächsten geplanten Agent-zu-Server-Kommunikation.

Verwalten von Agentensteuerungen

Sie können in Ihrem Netzwerk Agentensteuerungen einrichten und ihnen McAfee Agents zuweisen.

Aufgaben

- *Zuweisen von McAfee Agents zu Agentensteuerungen* auf Seite 102
  Sie können Agenten zu bestimmten Steuerungen zuweisen. Die Zuweisung von Systemen kann einzeln, nach der Gruppe oder nach dem Subnetz erfolgen.
- *Verwalten von Agentensteuerungszuweisungen* auf Seite 103
  Führen Sie die allgemeinen Verwaltungsausgaben für Agentensteuerungszuweisungen durch.
- *Erstellen von Agentensteuerungsgruppen* auf Seite 104
  Mithilfe von Steuerungsgruppen wird die Verwaltung mehrerer Steuerungen in einem Netzwerk vereinfacht. Außerdem können Steuerungsgruppen bei Ihrer Alternativstrategie eine Rolle spielen.
- *Verwalten von Agentensteuerungsgruppen* auf Seite 104
  Führen Sie die allgemeinen Verwaltungsausgaben für Agentensteuerungsgruppen durch.
- *Verschieben von Agenten zwischen Steuerungen* auf Seite 105
  Sie können Agenten zu bestimmten Steuerungen zuweisen. Die Zuweisung von Systemen kann mithilfe von Zuweisungsregeln oder der Zuweisungspriorität für Agentensteuerungen sowie individuell mithilfe der Systemstruktur erfolgen.

Zuweisen von McAfee Agents zu Agentensteuerungen

Sie können Agenten zu bestimmten Steuerungen zuweisen. Die Zuweisung von Systemen kann einzeln, nach der Gruppe oder nach dem Subnetz erfolgen.

Steuerungszuweisungen können angeben, ob eine einzelne Steuerung oder eine Liste von Steuerungen verwendet werden soll. Die von Ihnen angegebene Liste kann aus einzelnen Steuerungen oder Gruppen von Steuerungen bestehen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Konfiguration** | **Agentensteuerungen**, und klicken Sie dann auf **Aktionen** | **Neue Zuweisung**.

2 Geben Sie einen eindeutigen Namen für die Zuweisung an.

3 Geben Sie die Agenten für diese Zuweisung mithilfe der folgenden Optionen für **Agenten-Kriterien** an:

- Wechseln Sie zu einem **Speicherort in der Systemstruktur**.
- Geben Sie die IP-Adresse, den IP-Bereich oder die Subnetzmaske von verwalteten Systemen in das Feld **Agenten-Subnetz** ein.

4 Geben Sie die **Steuerungspriorität** mithilfe einer der beiden folgenden Optionen an:

- **Alle Agentensteuerungen verwenden** – Die Agenten wählen nach dem Zufallsprinzip aus, mit welcher Steuerung sie kommunizieren.
- **Liste benutzerdefinierter Steuerungen verwenden** – Wählen Sie bei Verwendung einer Liste benutzerdefinierter Steuerungen die Steuerung oder Steuerungsgruppe im Dropdown-Menü aus.

Bei Verwendung einer Liste benutzerdefinierter Steuerungen können Sie mit **+** und **-** weitere Agentensteuerungen hinzufügen bzw. entfernen (eine Agentensteuerung kann auch in mehreren Gruppen enthalten sein). Ändern Sie die Priorität von Steuerungen mittels Ziehen und Ablegen. Mit welcher Steuerung die Agenten die Kommunikation zuerst versuchen, richtet sich nach der Priorität.

Verwalten von Agentensteuerungszuweisungen

Führen Sie die allgemeinen Verwaltungsausgaben für Agentensteuerungszuweisungen durch.

Klicken Sie zum Durchführen dieser Aktionen auf **Menü** | **Konfiguration** | **Agentensteuerungen**, und klicken Sie dann in **Zuweisungsregeln für Steuerung** auf **Aktionen**.

Aktion	Vorgehensweise
Löschen einer Steuerungszuweisung	Klicken Sie in der Zeile mit der ausgewählten Zuweisung auf **Löschen**.
Bearbeiten einer Steuerungszuweisung	Klicken Sie für die ausgewählte Zuweisung auf **Bearbeiten**. Die Seite **Agentensteuerungszuweisung** wird geöffnet, auf der Sie Folgendes angeben können: • **Zuweisungsname** – Der eindeutige Name, mit dem diese Steuerungszuweisung identifiziert wird. • **Agenten-Kriterien** – Die Systeme, die in dieser Zuweisung enthalten sind. Sie können Systemstrukturgruppen hinzufügen und entfernen oder die Liste der Systeme im Textfeld ändern. • **Steuerungspriorität** – Wählen Sie aus, ob alle Agentensteuerungen oder eine Liste benutzerdefinierter Steuerungen verwendet werden soll. Wenn **Alle Agentensteuerungen verwenden** ausgewählt ist, wählen Agenten ihre Steuerung für die Kommunikation nach dem Zufallsprinzip aus. Mittels Ziehen und Ablegen können Sie die Priorität von Steuerungen in Ihrer Liste benutzerdefinierter Steuerungen schnell ändern.
Exportieren von Steuerungszuweisungen	Klicken Sie auf **Exportieren**. Die Seite **Agentensteuerungszuweisungen herunterladen** wird geöffnet, auf der Sie die Datei AGENTHANDLERASSIGNMENTS.XML anzeigen oder herunterladen können.
Importieren von Steuerungszuweisungen	Klicken Sie auf **Importieren**. Das Dialogfeld **Aktion: Importieren** wird geöffnet, in dem Sie zu einer zuvor heruntergeladenen Datei mit dem Namen AGENTHANDLERASSIGNMENTS.XML wechseln können.
Bearbeiten der Priorität von Steuerungszuweisungen	Klicken Sie auf **Priorität bearbeiten**. Die Seite **Agentensteuerungszuweisung** | **Priorität bearbeiten** wird geöffnet, auf der Sie die Priorität von Steuerungszuweisungen mittels Ziehen und Ablegen ändern.
Anzeigen einer Zusammenfassung der Details einer Steuerungszuweisung	Klicken Sie in der Zeile mit der ausgewählten Zuweisung auf **>**.

Erstellen von Agentensteuerungsgruppen

Mithilfe von Steuerungsgruppen wird die Verwaltung mehrerer Steuerungen in einem Netzwerk vereinfacht. Außerdem können Steuerungsgruppen bei Ihrer Alternativstrategie eine Rolle spielen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Konfiguration** | **Agenten-Handler** und dann unter **Handler-Gruppen** auf **Neue Gruppe**.

Die Seite Gruppe hinzufügen/bearbeiten wird angezeigt.

2 Geben Sie den Gruppennamen und die Details zu **Eingeschlossene Handler** an. Dazu gehören:

- Klicken Sie zum Verwenden eines Lastausgleichs von einem Drittanbieter auf **Lastausgleich verwenden**, und füllen Sie dann die Felder **Virtueller DNS-Name** und **Virtuelle IP-Adresse** aus (beide Felder sind erforderlich).
- Klicken Sie auf **Liste benutzerdefinierter Handler verwenden**, um die in dieser Gruppe enthaltenen Agenten-Handler anzugeben.

Bei Verwendung einer Liste benutzerdefinierter Handler wählen Sie die Handler in der Dropdown-Liste Eingeschlossene Handler aus. Mit **+** und **-** können Sie weitere Agenten-Handler zur Liste hinzufügen bzw. aus ihr entfernen (ein Agenten-Handler kann auch in mehreren Gruppen enthalten sein). Ändern Sie die Priorität von Handlern mithilfe von Ziehen und Ablegen. Mit welchem Handler die Kommunikation von den Agenten zuerst versucht wird, richtet sich nach der Priorität.

3 Klicken Sie auf **Speichern**.

Verwalten von Agentensteuerungsgruppen

Führen Sie die allgemeinen Verwaltungsausgaben für Agentensteuerungsgruppen durch.

Klicken Sie zum Durchführen dieser Aktionen auf **Menü** | **Konfiguration** | **Agentensteuerungen**, und klicken Sie dann auf den Monitor **Steuerungsgruppen**.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Aktionen	Vorgehensweise
Löschen einer Steuerungsgruppe	Klicken Sie in der Zeile mit der ausgewählten Gruppe auf **Löschen**.
Bearbeiten einer Steuerungsgruppe	Klicken Sie auf eine Steuerungsgruppe. Die Seite Einstellungen der Agentensteuerungsgruppe wird geöffnet. Dort können Sie Folgendes angeben: • **Virtueller DNS-Name** – Der eindeutige Name, mit dem diese Steuerungsgruppe identifiziert wird. • **Virtuelle IP-Adresse** – Die mit dieser Gruppe verknüpfte IP-Adresse. • **Eingeschlossene Steuerungen** – Wählen Sie aus, ob ein Drittanbieter-Lastausgleich oder eine Liste benutzerdefinierter Steuerungen verwendet werden soll. Mithilfe einer Liste benutzerdefinierter Steuerungen geben Sie an, mit welchen Steuerungen (und in welcher Reihenfolge) Agenten kommunizieren, die dieser Gruppe zugewiesen sind.
Aktivieren oder Deaktivieren einer Steuerungsgruppe	Klicken Sie in der Zeile mit der ausgewählten Gruppe auf **Aktivieren** bzw. **Deaktivieren**.

Verschieben von Agenten zwischen Steuerungen

Sie können Agenten zu bestimmten Steuerungen zuweisen. Die Zuweisung von Systemen kann mithilfe von Zuweisungsregeln oder der Zuweisungspriorität für Agentensteuerungen sowie individuell mithilfe der Systemstruktur erfolgen.

Steuerungszuweisungen können angeben, ob eine einzelne Steuerung oder eine Liste von Steuerungen verwendet werden soll. Die von Ihnen angegebene Liste kann aus einzelnen Steuerungen oder Gruppen von Steuerungen bestehen.

Aufgaben

- *Gruppieren von Agenten mithilfe von Agentensteuerungszuweisungen* auf Seite 105
  Sie können Agentensteuerungszuweisungen erstellen, um McAfee Agents in Gruppen zusammenzufassen.
- *Gruppieren von Agenten nach Zuweisungspriorität* auf Seite 106
  Fassen Sie Agenten in Gruppen zusammen, und weisen Sie sie einer Agentensteuerung zu, die Zuweisungspriorität verwendet.
- *Gruppieren von Agenten mithilfe der Systemstruktur* auf Seite 107
  Gruppieren Sie Agenten, und weisen Sie ihnen mithilfe der Systemstruktur eine Agentensteuerung zu.

Gruppieren von Agenten mithilfe von Agentensteuerungszuweisungen

Sie können Agentensteuerungszuweisungen erstellen, um McAfee Agents in Gruppen zusammenzufassen.

Steuerungszuweisungen können angeben, ob eine einzelne Steuerung oder eine Liste von Steuerungen verwendet werden soll. Die von Ihnen angegebene Liste kann aus einzelnen Steuerungen oder Gruppen von Steuerungen bestehen.

Beim Zuweisen von Agenten zu Agentensteuerungen sollten Sie auf geographische Nähe achten, um unnötigen Netzwerkverkehr zu vermeiden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Konfiguration** | **Agentensteuerungen**, und klicken Sie dann auf die erforderliche Regel unter **Zuweisungsregeln für Steuerung**.

Die Seite **Agentensteuerungszuweisung** wird angezeigt.

Wenn die Liste nur die Standardzuweisungsregeln enthält, müssen Sie eine neue Zuweisung erstellen.

2 Geben Sie in das Feld **Zuweisungsname** einen Namen ein.

3 Sie können **Agenten-Kriterien** nach dem Speicherort in der Systemstruktur, nach dem Agenten-Subnetz oder individuell wie folgt konfigurieren:

- Speicherort in der Systemstruktur – Wählen Sie die Gruppe unter **Speicherort in der Systemstruktur** aus.

  Sie können die Systemstruktur durchsuchen, um andere Gruppen aus **Systemstrukturgruppe auswählen** auszuwählen und angezeigte Systemstrukturgruppen mithilfe der Schaltflächen **+** und **-** hinzuzufügen bzw. zu entfernen.

- Agenten-Subnetz – Geben Sie die IP-Adressen, IP-Bereiche oder Subnetzmasken in das Textfeld ein.
- Individuell – Geben Sie die IPv4/IPv6-Adresse für ein bestimmtes System in das Textfeld ein.

4 Sie können für die **Steuerungspriorität** entweder **Alle Agentensteuerungen verwenden** oder **Liste benutzerdefinierter Steuerungen verwenden** auswählen. Wenn Sie auf **Liste benutzerdefinierter Steuerungen verwenden** klicken, können Sie die Steuerung wie folgt ändern:

- Sie können die zugewiesene Steuerung ändern, indem Sie eine weitere Steuerung zur Liste hinzufügen und die vorher zugewiesene Steuerung löschen.
- Sie können weitere Steuerungen zur Liste hinzufügen und die Priorität festlegen, die der Agent bei der Kommunikation mit den Steuerungen einhält.

Bei Verwendung einer Liste benutzerdefinierter Steuerungen können Sie mit **+** und **-** weitere Agentensteuerungen zur Liste hinzufügen bzw. aus ihr entfernen (eine Agentensteuerung kann auch in mehreren Gruppen enthalten sein). Ändern Sie die Priorität von Steuerungen mittels Ziehen und Ablegen. Mit welcher Steuerung die Agenten die Kommunikation zuerst versuchen, richtet sich nach der Priorität.

5 Klicken Sie auf **Speichern**.

Gruppieren von Agenten nach Zuweisungspriorität

Fassen Sie Agenten in Gruppen zusammen, und weisen Sie sie einer Agentensteuerung zu, die Zuweisungspriorität verwendet.

Steuerungszuweisungen können angeben, ob eine einzelne Steuerung oder eine Liste von Steuerungen verwendet werden soll. Die von Ihnen angegebene Liste kann aus einzelnen Steuerungen oder Gruppen von Steuerungen bestehen. In dieser Liste ist die Reihenfolge festgelegt, in der Agenten versuchen, mithilfe einer bestimmten Agentensteuerung zu kommunizieren.

Achten Sie beim Zuweisen von Systemen zu Agentensteuerungen auf geographische Nähe, um unnötigen Netzwerkverkehr zu vermeiden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Konfiguration** | **Agentensteuerungen**. Die Seite **Agentensteuerung** wird angezeigt.

Wenn die Liste nur die Standardzuweisungsregeln enthält, müssen Sie eine neue Zuweisung erstellen.

2 Bearbeiten Sie die Zuweisungen gemäß den in der Aufgabe *Gruppieren von Agenten mithilfe von Zuweisungsregeln* aufgeführten Schritten.

3 Ändern Sie bei Bedarf die Priorität oder Hierarchie der Zuweisungen, indem Sie auf **Aktionen** | **Priorität bearbeiten** klicken.

Durch Verschieben einer Zuweisung in eine niedrigere Priorität als eine andere Zuweisung entsteht eine Hierarchie, in der die niedrigere Zuweisung ein Teil der höheren Zuweisung ist.

4 Gehen Sie wie nachfolgend beschrieben vor, um die Priorität einer Zuweisung zu ändern, die links in der Spalte **Priorität** angezeigt wird:

- Per Ziehen und Ablegen – Ziehen Sie die Zeile mit der Zuweisung in der Spalte **Priorität** nach oben oder nach unten.
- Durch Klicken auf **Zum Anfang** – Klicken Sie im Schnellzugriff auf **Zum Anfang**, um die ausgewählte Zuweisung in die oberste Priorität zu verschieben.

5 Klicken Sie auf **Speichern**, wenn Sie die Prioritäten der Zuweisungen ordnungsgemäß konfiguriert haben.

Gruppieren von Agenten mithilfe der Systemstruktur

Gruppieren Sie Agenten, und weisen Sie ihnen mithilfe der Systemstruktur eine Agentensteuerung zu.

Steuerungszuweisungen können angeben, ob eine einzelne Steuerung oder eine Liste von Steuerungen verwendet werden soll. Die von Ihnen angegebene Liste kann aus einzelnen Steuerungen oder Gruppen von Steuerungen bestehen.

Achten Sie beim Zuweisen von Systemen zu Agentensteuerungen auf geographische Nähe, um unnötigen Netzwerkverkehr zu vermeiden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Systeme**.
2. Wechseln Sie in der Spalte **Systemstruktur** zu dem System oder zu der Gruppe, das bzw. die Sie verschieben möchten.
3. Ziehen Sie Systeme aus der aktuell konfigurierten Systemgruppe in die gewünschte Systemgruppe.
4. Klicken Sie auf **OK**.

Verwalten Ihrer Netzwerksicherheit

Damit Ihr Unternehmen vor Bedrohungen geschützt bleibt, ist es besonders wichtig, dass Ihre McAfee-Produkte immer mit den neuesten Sicherheitsinhalten aktualisiert werden. Mit McAfee ePO können Sie diese Aktualisierungen auf allen Systemen in Ihrem Netzwerk vornehmen.

Kapitel 9 *Systemstruktur*
Kapitel 10 *Tags*
Kapitel 11 *Agent-zu-Server-Kommunikation*
Kapitel 12 *Sicherheitsschlüssel*
Kapitel 13 *Software-Manager*
Kapitel 14 *Produktausbringung*
Kapitel 15 *Manuelle Verwaltung von Paketen und Aktualisierungen*
Kapitel 16 *Richtlinienverwaltung*
Kapitel 17 *Client-Tasks*
Kapitel 18 *Server-Tasks*
Kapitel 19 *Verwalten von SQL-Datenbanken*

9 Systemstruktur

Die Systemstruktur ist eine grafische Darstellung der Struktur Ihres verwalteten Netzwerks.

Mithilfe von ePolicy Orchestrator können Sie die Strukturierung der Systeme automatisieren und anpassen. Die von Ihnen festgelegte Organisationsstruktur hat Einfluss darauf, wie Sicherheitsrichtlinien im Netzwerk vererbt und erzwungen werden.

Die Systemstruktur können Sie mit einer der folgenden Methoden organisieren:

- Durch automatische Synchronisierung mit Ihrem Active Directory- oder NT-Domänen-Server
- Durch kriterienbasierte Sortierung, wobei Kriterien manuell oder automatisch auf Systeme angewendet werden
- Durch manuelle Organisation von der Konsole aus (mittels Ziehen und Ablegen)

Inhalt

- *Aufbau der Systemstruktur*
- *Überlegungen beim Planen der Systemstruktur*
- *Active Directory-Synchronisierung*
- *Typen der Active Directory-Synchronisierung*
- *NT-Domänensynchronisierung*
- *Kriterienbasierte Sortierung*
- *Erstellen und Auffüllen von Systemstrukturgruppen*
- *Verschieben von Systemen innerhalb der Systemstruktur*
- *Funktionsweise von Systeme übertragen*
- *Zusammenspiel der Funktion für automatische Antworten mit der Systemstruktur*

Aufbau der Systemstruktur

Die Systemstruktur ist eine hierarchische Struktur, die die Systeme im Netzwerk in Gruppen und Untergruppen organisiert.

Standardmäßig enthält die Systemstruktur die folgenden *Gruppen*:

- **Eigenes Unternehmen** – Der Stamm der Systemstruktur.
- **Meine Gruppe**: Die Standardgruppe, die mit den ersten Schritten der Erstinstallation der Software hinzugefügt wird.

  Der Gruppenname könnte während der Erstinstallation der Software vom Standard geändert worden sein.

- **Sammelgruppe** – Die Erfassungsgruppe für alle Systeme, die nicht zu anderen Gruppen in der Systemstruktur gehören.

Gruppe Eigenes Unternehmen

Die Stammgruppe der Systemstruktur, Eigenes Unternehmen, enthält alle Systeme, die ihr (manuell oder automatisch) hinzugefügt oder im Netzwerk entdeckt wurden.

Bis Sie eine eigene Struktur erstellen, werden alle Systeme standardmäßig zu Meine Gruppe hinzugefügt.

Der Name Meine Gruppe könnte während der Erstinstallation der Software vom Standard geändert worden sein.

Die Gruppe Eigenes Unternehmen hat die folgenden Eigenschaften:

- Sie kann nicht gelöscht werden.
- Sie kann nicht umbenannt werden.

Meine Gruppe

Meine Gruppe ist eine Untergruppe der Gruppe Eigenes Unternehmen und wird standardmäßig während der Ersten Schritte der Erstinstallation der Software hinzugefügt.

Der Name Meine Gruppe könnte während der Erstinstallation der Software vom Standard geändert worden sein.

Wenn die Installations-URL auf Ihren Netzwerkcomputern ausgeführt wird, werden diese standardmäßig in Meine Gruppe der Systemstruktur gruppiert.

Klicken Sie auf **Systemstruktur** | **Aktionen**, um Meine Gruppe in der Systemstruktur zu löschen oder umzubenennen.

Denken Sie beim Entfernen von Systemen aus der Systemstruktur daran, die Option zum Entfernen der zugehörigen Agenten auszuwählen. Wenn McAfee Agent nicht entfernt wird, werden gelöschte Systeme erneut in der Gruppe Sammelgruppe angezeigt, da weiterhin zwischen McAfee Agent und McAfee ePO Cloud kommuniziert wird.

Sammelgruppe

Die Sammelgruppe ist eine Untergruppe der Gruppe Eigenes Unternehmen.

Abhängig von den Methoden, die Sie bei der Erstellung und Verwaltung der Systemstruktur angegeben haben, wird für den Server anhand unterschiedlicher Eigenschaften bestimmt, wo Systeme eingeordnet werden sollen. In der Sammelgruppe werden Systeme gespeichert, deren Standort nicht ermittelt werden konnte.

Die Sammelgruppe hat folgende Eigenschaften:

- Sie kann nicht gelöscht werden.
- Sie kann nicht umbenannt werden.
- Ihre Sortierungskriterien können nicht so geändert werden, dass sie keine Erfassungsgruppe mehr ist. Sie können jedoch Sortierungskriterien für die untergeordneten Untergruppen festlegen.
- Sie wird immer als letztes Element in der Systemstruktur angezeigt und innerhalb gleichrangiger Elemente nicht alphabetisch geordnet.

- Benutzern müssen Berechtigungen für die Sammelgruppe gewährt werden, damit sie die Inhalte dieser Gruppe anzeigen können.
- Wenn ein System in die Sammelgruppe sortiert wird, wird es in einer Untergruppe abgelegt, die nach der Domäne des Systems benannt ist. Falls diese Gruppe noch nicht vorhanden ist, wird sie erstellt.

Denken Sie beim Entfernen von Systemen aus der Systemstruktur daran, die Option zum Entfernen der zugehörigen Agenten auszuwählen. Falls McAfee Agent nicht entfernt wird, werden gelöschte Systeme in der Sammelgruppe wieder angezeigt, weil weiterhin eine Kommunikation zwischen McAfee Agent und dem Server stattfindet.

Systemstrukturgruppen

Systemstrukturgruppen stellen eine Sammlung von Systemen dar. Die Entscheidung, welche Systeme in eine Gruppe zusammengefasst werden sollen, hängt von den spezifischen Anforderungen Ihres Netzwerks und Unternehmens ab.

Sie können Systeme nach verschiedenen Kriterien zusammenfassen: nach dem Computertyp (z. B. Laptops, Server oder Desktop-PCs), nach der Region (z. B. Nordamerika oder Europa), nach unterschiedlichen Abteilungen (z. B. Finanzen oder Entwicklung) oder nach anderen Kriterien.

Gruppen können sowohl Systeme als auch andere Gruppen (*Untergruppen*) enthalten.

Gruppen haben folgende Eigenschaften:

- Sie werden von Administratoren oder Benutzern mit den entsprechenden Berechtigungen erstellt.
- Sie können sowohl Systeme als auch andere Gruppen (*Untergruppen*) enthalten.
- Sie werden von einem Administrator oder einem Benutzer mit den entsprechenden Berechtigungen verwaltet.

Durch das Gruppieren von Systemen mit ähnlichen Eigenschaften oder Anforderungen in Einheiten können Sie Richtlinien für Systeme zentral verwalten, anstatt die Richtlinien für jedes einzelne System individuell festzulegen.

Zur optimalen Planung sollten Sie Ihre Systeme in Gruppen organisieren, bevor Sie mit dem Erstellen der Systemstruktur beginnen.

Vererbung

Vererbung ist eine wichtige Eigenschaft, die das Verwalten von Richtlinien und Tasks vereinfacht. Durch Vererbung übernehmen in der Systemstrukturhierarchie untergeordnete Gruppen Richtlinien, die für ihre übergeordneten Gruppen festgelegt wurden.

Beispiel:

- Richtlinien, die in der Systemstruktur auf der Ebene Eigenes Unternehmen festgelegt wurden, werden an darunter liegende Gruppen vererbt.
- Untergruppen oder einzelne Systeme erben die Richtlinien ihrer Gruppen.

Die Vererbung ist standardmäßig für alle Gruppen und einzelnen Systeme aktiviert, die Sie der Systemstruktur hinzufügen. Dadurch müssen Sie an weniger Punkten Richtlinien festlegen und Client-Tasks planen.

Die Vererbung kann bei Bedarf durch Zuordnen einer neuen Richtlinie an einer beliebigen Stelle der Systemstruktur unterbrochen werden. Zur Beibehaltung der Vererbung können Sie Richtlinienzuweisungen sperren.

Überlegungen beim Planen der Systemstruktur

Eine effiziente und gut organisierte Systemstruktur kann die Wartung vereinfachen. Der Aufbau der Systemstruktur wird von vielen administrativen, netzwerkbedingten und politischen Gegebenheiten einer Umgebung beeinflusst.

Planen Sie daher den Aufbau der Systemstruktur, bevor Sie sie erstellen und auffüllen. Besonders bei großen Netzwerken wäre der Aufwand für das mehrfache Erstellen der Systemstruktur erheblich.

Da jedes Netzwerk anders ist und unterschiedliche Richtlinien erfordert (möglicherweise sogar eine unterschiedliche Verwaltung), empfiehlt McAfee, vor dem Hinzufügen der Systeme die Systemstruktur zu planen.

Unabhängig von den Methoden, die Sie zum Erstellen und Auffüllen der Systemstruktur verwenden, sollten Sie beim Planen der Systemstruktur die jeweilige Umgebung berücksichtigen.

Administratorzugriff

Wenn Sie die Organisation der Systemstruktur planen, sollten Sie die Anforderungen an den Benutzerzugriff der Personen berücksichtigen, die das System verwalten werden.

Möglicherweise verfügt Ihr Unternehmen über eine dezentralisierte Netzwerkverwaltung, bei der unterschiedliche Administratoren die Verantwortung für unterschiedliche Teile des Netzwerks tragen. Aus Sicherheitsgründen dürfen Sie möglicherweise kein Administratorkonto verwenden, das Zugriff auf alle Teile Ihres Netzwerks hat. In diesem Szenario dürfen Sie mit einem einzelnen Administratorkonto keine Richtlinien festlegen und keine Agenten ausbringen. Stattdessen müssen Sie die Systemstruktur möglicherweise auf Grundlage der Abteilungen in Gruppen organisieren und Konten und Berechtigungssätze erstellen.

Berücksichtigen Sie die folgenden Fragen:

- Wer ist für die Verwaltung welcher Systeme verantwortlich?
- Wer benötigt Zugriff auf Informationen zu diesen Systemen?
- Wer sollte Zugriff auf die Systeme und die Informationen dazu besitzen?

Diese Fragen haben sowohl Einfluss auf die Organisation der Systemstruktur als auch auf die Berechtigungssätze, die Sie erstellen und auf Benutzerkonten anwenden.

Gliederung der Umgebung und ihr Einfluss auf die Systemorganisation

Die Art der Organisation der Systeme für die Verwaltung hängt von der Gliederung Ihres Netzwerks ab. Diese Gliederung beeinflusst den Aufbau der Systemstruktur auf andere Weise als den Aufbau der Netzwerktopologie.

Sie sollten folgende Gliederungsarten im Netzwerk und im Unternehmen beurteilen und sich die Frage stellen, ob diese beim Aufbau der Systemstruktur berücksichtigt werden müssen.

Topologische Gliederung

Mit NT-Domänen oder Active Directory-Containern definieren Sie das Netzwerk. Je besser die Netzwerkumgebung organisiert ist, desto einfacher ist es, die Systemstruktur mit den Synchronisierungsfunktionen zu erstellen und zu verwalten.

Geographische Gliederung

Die Verwaltung der Sicherheit ist eine ständige Balance zwischen Schutz und Leistung. Bauen Sie die Systemstruktur so auf, dass die begrenzte Bandbreite bestmöglich genutzt wird. Überprüfen Sie, wie die Verbindung zwischen dem Server und den Teilen des Netzwerks hergestellt wird. Vor allem

Remote-Standorte sind oft nur über langsame WAN- oder VPN-Verbindungen statt über schnellere LAN-Verbindungen angeschlossen. Um den Netzwerkverkehr über langsamere Verbindungen zu verringern, sollten Sie Richtlinien für Aktualisierung und Agent-Server-Kommunikation für Remote-Standorte anders konfigurieren.

Politische Gliederung

Viele große Netzwerke sind nach Personen oder Gruppen unterteilt, die unterschiedliche Teile des Netzwerks verwalten. Manchmal stimmt diese Gliederung nicht mit der topologischen oder geografischen Gliederung überein. Die Auswahl der Personen, die auf die Segmente der Systemstruktur zugreifen und sie verwalten, beeinflusst deren Strukturierung.

Funktionale Gliederung

Einige Netzwerke werden nach den Rollen der Netzwerkbenutzer unterteilt, zum Beispiel die Vertriebs- und die Entwicklungsabteilung. Selbst wenn das Netzwerk nicht funktional gegliedert ist, müssen Sie Teile der Systemstruktur möglicherweise nach Funktion organisieren, wenn verschiedene Gruppen unterschiedliche Richtlinien benötigen.

Eine Geschäftsgruppe verwendet möglicherweise spezifische Software, für die spezielle Sicherheitsrichtlinien erforderlich sind. Sie können zum Beispiel die E-Mail-Exchange-Server in einer Gruppe anordnen und bestimmte Ausschlüsse für On-Access-Scans festlegen.

Subnetze und IP-Adressbereiche

In vielen Fällen werden für Organisationseinheiten eines Netzwerks bestimmte Subnetze oder IP-Bereiche verwendet, weshalb Sie für einen geographischen Standort eine Gruppe erstellen und mindestens einen IP-Filter dafür festlegen können. Wenn Ihr Netzwerk jedoch nicht über mehrere geographische Standorte verteilt ist, können Sie als primäres Gliederungskriterium Informationen zum Netzwerkstandort verwenden, z. B. IP-Adressen.

Sie sollten nach Möglichkeit auf IP-Adressinformationen basierende Sortierungskriterien zur Automatisierung der Systemstrukturerstellung und -wartung verwenden. Legen Sie Kriterien für IP-Subnetzmasken oder IP-Adressbereiche für mögliche Gruppen in der Systemstruktur fest. Diese Filter füllen Speicherorte automatisch mit den entsprechenden Systemen auf.

Betriebssysteme und Software

Systeme mit ähnlichen Betriebssystemen können Sie in Gruppen zusammenfassen, um das Verwalten betriebssystemspezifischer Produkte und Richtlinien zu vereinfachen. Wenn Sie über ältere Systeme verfügen, können Sie dafür eine Gruppe erstellen und Sicherheitsprodukte auf diesen Systemen separat ausbringen und verwalten. Indem Sie diesen Systemen ein entsprechendes Tag zuweisen, können Sie sie außerdem automatisch in eine Gruppe sortieren.

Tags und Systeme mit ähnlichen Eigenschaften

Mit Tags und Tag-Gruppen können Sie das Sortieren in Gruppen automatisieren.

Tags identifizieren Systeme mit ähnlichen Eigenschaften. Wenn Sie die Gruppen anhand von Eigenschaften organisieren können, haben Sie die Möglichkeit, auf diesen Kriterien basierende Tags zu erstellen und zuzuordnen und diese Tags als Gruppensortierungskriterien zu verwenden. Auf diese Weise stellen Sie sicher, dass die Systeme automatisch in die entsprechenden Gruppen sortiert werden.

Verwenden Sie nach Möglichkeit Tag-basierte Sortierungskriterien, um die Gruppen automatisch mit den entsprechenden Systemen aufzufüllen. Darüber hinaus können Sie die Sortierung der Systeme erleichtern, indem Sie verschachtelte Tag-Gruppen mit bis zu vier Ebenen erstellen, die jeweils bis zu 1.000 Tag-Untergruppen enthalten. Wenn Sie die Systeme beispielsweise nach dem geografischen

Standort, dem Chassis-Typ (Server, Workstation oder Laptop), der Systemfunktion (Web-Server, SQL-Server oder Anwendungs-Server) und dem Benutzer organisieren, verwenden Sie möglicherweise die folgenden Tag-Gruppen:

Standort	Chassis-Typ	Plattform	Benutzer
Los Angeles	Desktop-PC	Windows	Allgemein
	Laptop	Macintosh	Vertrieb
			Schulung
		Windows	Buchhaltung
			Verwaltung
	Server	Linux	Unternehmen
		Windows	Unternehmen
		SQL	Unternehmen
San Francisco	Desktop-PC	Windows	Allgemein
	Laptop	Macintosh	Vertrieb
			Schulung
		Windows	Buchhaltung
			Verwaltung
	Server	Linux	Unternehmen
		Windows	Unternehmen
		SQL	Unternehmen

Active Directory-Synchronisierung

Wenn im Netzwerk Active Directory ausgeführt wird, können Sie Teile der Systemstruktur mit der Active Directory-Synchronisierung erstellen, auffüllen und verwalten.

Nachdem die Systemstruktur definiert wurde, wird sie mit neuen Systemen (und Untercontainern) in Active Directory aktualisiert.

Nutzen Sie die Active Directory-Integration, um die folgenden Systemverwaltungsaufgaben auszuführen:

- Synchronisieren mit der Active Directory-Struktur durch Importieren von Systemen und Active Directory-Untercontainern (als Systemstrukturgruppen) sowie Aktualisieren mit Active Directory. Bei jeder Synchronisierung werden die Systeme und die Struktur in der Systemstruktur aktualisiert, um die Systeme und die Struktur von Active Directory widerzuspiegeln.
- Importieren von Systemen als unsortierte Liste aus dem Active Directory-Container (und seinen Untercontainern) in die synchronisierte Gruppe.
- Steuern der Vorgehensweise bei potenziell doppelten Systemen.
- Verwenden der Systembeschreibung, die zusammen mit den Systemen aus Active Directory importiert wird.

Gehen Sie wie nachfolgend beschrieben vor, um die Systemstruktur in die Active Directory-Systemstruktur zu integrieren:

1 Konfigurieren Sie die Synchronisierungseinstellungen in jeder Gruppe, die einen Zuordnungspunkt in der Systemstruktur darstellt. An der gleichen Stelle können Sie konfigurieren, ob Folgendes möglich sein soll:
   - Agenten auf entdeckte Systeme ausgebracht werden sollen.
   - Löschen von Systemen in der Systemstruktur, wenn diese in Active Directory gelöscht werden
   - Doppelte Einträge von Systemen, die an einer anderen Stelle in der Systemstruktur vorhanden sind

2 Importieren Sie die Active Directory-Systeme (und gegebenenfalls die Struktur) entsprechend den Synchronisierungseinstellungen mit der Aktion **Jetzt synchronisieren** in die Systemstruktur.

3 Verwenden Sie den Server-Task NT-Domänen-/Active Directory-Synchronisierung, um die Systeme (und gegebenenfalls die Active Directory-Struktur) entsprechend den Synchronisierungseinstellungen regelmäßig mit der Systemstruktur zu synchronisieren.

Typen der Active Directory-Synchronisierung

Es gibt zwei Typen der Active Directory-Synchronisierung (*Nur Systeme* sowie *Systeme und Struktur*). Je nachdem, wie weit Sie Active Directory integrieren möchten, können Sie sich für eine Variante entscheiden.

Bei beiden Typen steuern Sie die Synchronisierung durch die Auswahl folgender Optionen:

- Automatisches Ausbringen von Agenten auf Systemen, die in ePolicy Orchestrator neu sind. Diese Einstellung sollten Sie nicht für die erste Synchronisierung festlegen, wenn Sie eine große Anzahl an Systemen importieren und nur eine begrenzte Bandbreite zur Verfügung steht. Die Agenten-MSI-Datei hat eine Größe von ca. 6 MB. Möglicherweise möchten Sie Agenten jedoch bei späteren Synchronisierungen automatisch auf neuen Systemen ausbringen, die in Active Directory erkannt werden.
- Löschen von Systemen von ePolicy Orchestrator (und entfernen ihrer Agenten), wenn sie in Active Directory gelöscht werden.
- Verhindern, dass Systeme zur Gruppe hinzugefügt werden, wenn sie bereits an einer anderen Stelle der Systemstruktur vorhanden sind. Damit stellen Sie sicher, dass beim manuellen Verschieben oder Sortieren von Systemen keine doppelten Systeme erstellt werden.
- Ausschließen bestimmter Active Directory-Container aus der Synchronisierung. Diese Container und ihre Systeme werden bei der Synchronisierung ignoriert.

Systeme und Struktur

Wenn Sie diesen Synchronisierungstyp verwenden, werden Änderungen an der Active Directory-Struktur bei der nächsten Synchronisierung in die Systemstruktur übernommen. Beim Hinzufügen, Ändern oder Entfernen von Systemen oder Containern in Active Directory werden diese an den entsprechenden Stellen der Systemstruktur ebenfalls hinzugefügt, geändert oder entfernt.

Verwendung dieses Synchronisierungstyps

Mithilfe dieses Synchronisierungstyps stellen Sie sicher, dass die Systemstruktur (oder Teile davon) Ihrer Active Directory-Struktur genau gleichen.

Wenn die Organisation von Active Directory Ihre Anforderungen an die Sicherheitsverwaltung erfüllt und die Systemstruktur weiterhin der zugewiesenen Active Directory-Struktur gleichen soll, verwenden Sie diesen Synchronisierungstyp bei nachfolgenden Synchronisierungen.

Nur Systeme

Mit diesem Synchronisierungstyp können Sie Systeme aus einem Active Directory-Container (und aus nicht ausgeschlossenen Untercontainern) als unsortierte Liste in eine zugewiesene Systemstrukturgruppe importieren. Anschließend können Sie die Systeme an die entsprechenden Stellen in der Systemstruktur verschieben, indem Sie Gruppen Sortierungskriterien zuweisen.

Wenn Sie sich für diesen Synchronisierungstyp entscheiden, müssen Sie sich vergewissern, dass Sie keine Systeme erneut hinzufügen, die bereits an einer anderen Stelle in der Systemstruktur vorhanden sind. Auf diese Weise vermeiden Sie doppelte Einträge in der Systemstruktur.

Verwendung dieses Synchronisierungstyps

Verwenden Sie diesen Synchronisierungstyp, wenn Sie Active Directory als Standardquelle für ePolicy Orchestrator verwenden und die Unternehmensanforderungen an die Sicherheitsverwaltung sich nicht mit der Organisation der Container und Systeme in Active Directory vereinbaren lassen.

NT-Domänensynchronisierung

Verwenden Sie Ihre NT-Domänen als Ausgangspunkt für das Auffüllen der Systemstruktur. Wenn Sie eine Gruppe mit einer NT-Domäne synchronisieren, werden alle Systeme dieser Domäne als unsortierte Liste in der Gruppe abgelegt. Sie können diese Systeme in einer einzelnen Gruppe verwalten oder zur genaueren Gliederung Untergruppen erstellen. Mithilfe einer Methode wie der automatischen Sortierung können Sie diese Untergruppen automatisch auffüllen.

Wenn Sie Systeme in andere Gruppen oder Untergruppen der Systemstruktur verschieben, stellen Sie sicher, dass Sie die Systeme nicht hinzufügen, wenn sie an anderer Stelle der Systemstruktur bereits vorhanden sind. Auf diese Weise vermeiden Sie doppelte Einträge in der Systemstruktur.

Anders als bei der Active Directory-Synchronisierung werden bei der NT-Domänensynchronisierung nur die Systemnamen synchronisiert. Die Systembeschreibung wird nicht synchronisiert.

Kriterienbasierte Sortierung

Sie können IP-Adressinformationen verwenden, um verwaltete Systeme automatisch in bestimmte Gruppen zu sortieren. Sie können auch Tag-basierte Sortierungskriterien erstellen, die Systemen zugewiesenen Beschriftungen ähneln. Um sicherzustellen, dass sich Systeme an der gewünschten Stelle in der Systemstruktur befinden, können Sie entweder einen der Kriterientypen oder beide verwenden.

Systeme müssen nur ein Kriterium der Sortierungskriterien einer Gruppe erfüllen, um der Gruppe zugeordnet zu werden.

Führen Sie nach dem Erstellen von Gruppen und dem Festlegen Ihrer Sortierungskriterien einen Sortiertest aus, um zu überprüfen, ob die Kriterien und die Sortierreihenfolge die gewünschten Ergebnisse erzielen.

Sobald Sie Sortierungskriterien zu den Gruppen hinzugefügt haben, können Sie die Aktion Jetzt sortieren ausführen. Mit dieser Aktion werden die ausgewählten Systeme automatisch in die entsprechende Gruppe verschoben. Systeme, die den Sortierungskriterien keiner Gruppe entsprechen, werden in die Sammelgruppe verschoben.

Neue Systeme, die sich zum ersten Mal beim Server anmelden, werden automatisch zur richtigen Gruppe hinzugefügt. Wenn Sie die Sortierungskriterien jedoch nach der ersten Agent-Server-Kommunikation definieren, müssen Sie für diese Systeme die Aktion Jetzt sortieren ausführen, um sie sofort in die entsprechende Gruppe zu verschieben. Sie können jedoch auch bis zur nächsten Agent-Server-Kommunikation warten.

Sortierungsstatus der Systeme

Sie können die Systemstruktursortierung für jedes System oder für jede Sammlung von Systemen aktivieren bzw. deaktivieren. Wenn Sie die Systemstruktursortierung bei einem System deaktivieren, wird es von allen Sortieraktionen bis auf die **Testsortierung** ausgeschlossen. Bei der Testsortierung wird der Sortierungsstatus des Systems oder der Sammlung betrachtet, und das System kann auf der Seite Testsortierung verschoben oder sortiert werden.

Einstellungen der Systemstruktursortierung auf dem McAfee ePO-Server

Die Sortierung kann nur ausgeführt werden, wenn die Sortierfunktion auf dem Server und auf den Systemen aktiviert ist. Standardmäßig ist das einmalige Sortieren von Systemen aktiviert. Daher werden Systeme bei der ersten Agent-zu-Server-Kommunikation (oder dann, wenn an vorhandenen Systemen Änderungen vorgenommen werden) sortiert, und danach nicht wieder.

Systemsortiertest

Mit dieser Funktion können Sie anzeigen, wo Systeme bei einer Sortierungsaktion abgelegt werden würden. Auf der Seite **Sortiertest** werden die Systeme und die Pfade der Speicherorte angezeigt, an denen sie einsortiert werden würden. Zwar wird der Sortierungsstatus der Systeme auf dieser Seite nicht angezeigt, doch wenn Sie Systeme auf der Seite auswählen (selbst solche mit deaktivierter Sortierung) und auf **Systeme verschieben** klicken, werden die Systeme am angegebenen Speicherort abgelegt.

Auswirkung von Einstellungen auf die Sortierung

Sie können zwischen drei Server-Einstellungen wählen, die bestimmen, ob und wann Systeme sortiert werden. Außerdem können Sie auswählen, ob ein System sortiert werden kann, indem Sie die Systemstruktursortierung für ausgewählte Systeme in der Systemstruktur aktivieren oder deaktivieren.

Server-Einstellungen

Der Server verfügt über drei Einstellungen:

- **Systemstruktursortierung deaktivieren**: Wenn eine kriterienbasierte Sortierung Ihre Anforderungen an die Sicherheitsverwaltung nicht erfüllt und Sie die Systeme mit anderen Systemstrukturfunktionen organisieren möchten, wählen Sie diese Einstellung aus, damit andere ePolicy Orchestrator-Benutzer nicht versehentlich Sortierungskriterien für Gruppen konfigurieren und Systeme an unerwünschte Speicherorte verschieben.
- **Systeme bei jeder Agent-zu-Server-Kommunikation sortieren** – Die Systeme werden bei jeder Agent-zu-Server-Kommunikation erneut sortiert. Wenn Sie die Sortierungskriterien für Gruppen ändern, werden die Systeme bei der nächsten Agent-zu-Server-Kommunikation in die neue Gruppe verschoben.
- **Systeme einmal sortieren** – Die Systeme werden bei der nächsten Agent-zu-Server-Kommunikation sortiert und dann gekennzeichnet, sodass sie bei Agent-zu-Server-Kommunikationen nicht mehr sortiert werden, so lange diese Einstellung ausgewählt ist. Sie können ein solches System jedoch sortieren, indem Sie es markieren und auf **Jetzt sortieren** klicken.

Systemeinstellungen

Sie können die Systemstruktursortierung für jedes System deaktivieren oder aktivieren. Wenn die Systemstruktursortierung auf einem System deaktiviert ist, wird dieses unabhängig von der ausgeführten Sortierungsaktion nicht sortiert. Bei der **Testsortierung** wird das System jedoch sortiert. Bei aktivierter Systemstruktursortierung wird das betreffende System bei der manuellen Aktion **Jetzt sortieren** und (je nach den Server-Einstellungen für die Systemstruktursortierung) bei der Agent-Server-Kommunikation sortiert.

Kriterien für die IP-Adressensortierung

In vielen Netzwerken geben die Subnetze und IP-Adressinformationen Hinweise auf die Unternehmensstruktur (z. B. auf geographische Standorte oder Aufgaben). Wenn die Organisation der IP-Adressen Ihren Anforderungen entspricht, sollten Sie die Systemstruktur oder Teile davon mithilfe dieser Informationen erstellen und verwalten, indem Sie Kriterien für die IP-Adressensortierung für solche Gruppen festlegen.

In der vorliegenden Version von ePolicy Orchestrator wurde diese Funktion geändert, und Sie haben jetzt die Möglichkeit, IP-Sortierungskriterien an jedem beliebigen Punkt in der Struktur festzulegen. Sie müssen nicht mehr darauf achten, dass die Kriterien der IP-Adressensortierung der untergeordneten Gruppe eine Teilmenge der Kriterien der übergeordneten Gruppe sind (sofern der übergeordneten Gruppe keine Kriterien zugewiesen sind). Sobald die Funktion konfiguriert ist, können Sie Systeme bei einer Agent-zu-Server-Kommunikation oder nur bei einer manuell ausgelösten Sortierungsaktion sortieren.

Die Kriterien für die IP-Adressensortierung sollten sich zwischen den einzelnen Gruppen nicht überschneiden. Jeder IP-Bereich oder jede IP-Subnetzmaske in den Sortierungskriterien einer Gruppe sollte eine eindeutige Menge an IP-Adressen abdecken. Wenn sich Kriterien überschneiden, hängt es von der Reihenfolge der Untergruppen auf der Registerkarte **Systemstruktur** | **Gruppeninformationen** ab, in welche Gruppe diese Systeme sortiert werden. Mit der Aktion **IP-Integrität überprüfen** auf der Registerkarte **Gruppeninformationen** können Sie IP-Adressen auf Überscheidungen überprüfen.

Tag-basierte Sortierungskriterien

Sie können nicht nur Systeme mithilfe von IP-Adressinformationen in die entsprechende Gruppe sortieren, sondern auch Sortierungskriterien anhand der den Systemen zugewiesenen Tags definieren.

Tag-basierte Kriterien können zusammen mit auf IP-Adressen basierenden Kriterien für die Sortierung genutzt werden.

Gruppenreihenfolge und -sortierung

Zusätzliche Flexibilität bei der Systemstrukturverwaltung erhalten Sie, indem Sie die Reihenfolge der Untergruppen einer Gruppe konfigurieren. Damit legen Sie auch die Reihenfolge fest, in der diese Untergruppen beim Sortieren für eine Einordnung des Systems in Betracht gezogen werden.

Wenn mehrere Untergruppen übereinstimmende Kriterien besitzen, kann die Änderung dieser Reihenfolge die Position eines Systems in der Systemstruktur ändern.

Wenn Sie Erfassungsgruppen verwenden, müssen diese außerdem die letzte Untergruppe in der Liste sein.

Erfassungsgruppen

Bei Erfassungsgruppen handelt es sich um Gruppen, deren Sortierungskriterien auf der Seite **Sortierungskriterien** der Gruppe auf **Alle anderen** eingestellt sind. Nur Untergruppen an der letzten Stelle der Sortierreihenfolge können Erfassungsgruppen sein. Diese Gruppen erhalten alle Systeme, die in die übergeordnete Gruppe, aber in keine der gleichrangigen Gruppen der Erfassungsgruppe sortiert wurden.

Hinzufügen eines Systems zur Systemstruktur bei aktivierter Sortierung

Bei der ersten Kommunikation zwischen McAfee Agent und dem Server wird das System vom Server mithilfe eines Algorithmus in die Systemstruktur eingeordnet. Systeme, für die kein geeigneter Speicherort gefunden wird, werden in der Sammelgruppe abgelegt.

Bei jeder Agent-Server-Kommunikation wird das System vom Server anhand der McAfee Agent-GUID in der Systemstruktur gesucht. (Nur Systeme, deren Agenten sich bereits zum ersten Mal beim Server gemeldet haben, verfügen über eine McAfee Agent-GUID in der Datenbank.) Falls ein übereinstimmendes System gefunden wird, verbleibt es in seinem vorhandenen Speicherort.

Wenn kein übereinstimmendes System gefunden wird, werden die Systeme vom Server mithilfe eines Algorithmus in die entsprechenden Gruppen sortiert. Die Systeme können in eine beliebige kriterienbasierte Gruppe in der Systemstruktur eingeordnet werden. Dabei spielt es keine Rolle, wie tief die Gruppe in der Struktur angeordnet ist. Voraussetzung dafür ist, dass die Kriterien aller übergeordneten Gruppen des Pfads übereinstimmen. Übergeordnete Gruppen einer kriterienbasierten Untergruppe müssen entweder keine Kriterien oder übereinstimmende Kriterien haben.

Die den einzelnen Untergruppen zugewiesene Sortierreihenfolge (die auf der Registerkarte **Gruppeninformationen** definiert ist) bestimmt, in welcher Reihenfolge diese Untergruppen vom Server berücksichtigt werden, wenn nach einer Gruppe mit übereinstimmenden Kriterien gesucht wird.

1. Vom Server wird in einer Gruppe, die den gleichen Namen wie die Domäne trägt, nach einem System ohne McAfee Agent-GUID (McAfee Agent hat sich noch nie gemeldet) mit einem übereinstimmenden Namen gesucht. Wenn ein System gefunden wird, wird es in diese Gruppe eingeordnet. Dieser Vorgang kann bei der ersten Active Directory- oder NT-Domänensynchronisierung oder beim manuellen Hinzufügen von Systemen zur Systemstruktur erfolgen.
2. Wenn kein übereinstimmendes System gefunden wird, sucht der Server nach einer Gruppe, die denselben Namen wie die Domäne trägt, aus der das System stammt. Wird keine solche Gruppe gefunden, wird sie innerhalb der Lost&Found-Gruppe erstellt, und das System wird zu dieser Gruppe hinzugefügt.
3. Die Eigenschaften des Systems werden aktualisiert.
4. Wenn der Server so konfiguriert ist, dass er die Sortierungskriterien bei jeder Agent-zu-Server-Kommunikation ausführt, wendet er alle kriterienbasierten Tags auf das System an.
5. Die weiteren Schritte hängen davon ab, ob die Systemstruktursortierung sowohl auf dem Server als auch auf dem System aktiviert ist.
   - Wenn die Systemstruktursortierung entweder auf dem Server oder dem System deaktiviert ist, wird das System an seinem derzeitigen Speicherort belassen.
   - Wenn die Systemstruktursortierung auf dem Server und dem System aktiviert ist, wird das System basierend auf den Sortierungskriterien in die Systemstrukturgruppen verschoben.

   Bei Systemen, die während der Active Directory- oder NT-Domänensynchronisierung hinzugefügt wurden, ist die Systemstruktursortierung standardmäßig deaktiviert, sodass sie bei der ersten Agent-Server-Kommunikation nicht sortiert werden.
6. Die Sortierungskriterien aller Gruppen der obersten Ebene werden vom Server entsprechend der Sortierreihenfolge auf der Registerkarte **Gruppeninformationen** der Gruppe Eigenes Unternehmen

berücksichtigt. Das System wird vom Server zur ersten Gruppe mit übereinstimmenden Kriterien oder zu einer Erfassungsgruppe zugeordnet, die er berücksichtigt.

- Sobald ein System einer Gruppe zugeordnet ist, werden alle seine Untergruppen entsprechend ihrer Sortierreihenfolge auf der Registerkarte Gruppeninformationen auf übereinstimmende Kriterien überprüft.
- Dieser Vorgang wird so lange ausgeführt, bis keine Untergruppe mit übereinstimmenden Kriterien für das System vorhanden ist und es der letzten gefundenen Gruppe mit übereinstimmenden Kriterien zugeordnet wird.

7 Wenn keine übergeordnete Gruppe gefunden wird, werden die Untergruppen von übergeordneten Gruppen (ohne Sortierungskriterien) entsprechend ihrer Sortierung berücksichtigt.

8 Wenn keine solche kriterienbasierte Gruppe der zweiten Ebene gefunden wird, werden die kriterienbasierten Gruppen der dritten Ebene aus den uneingeschränkten Gruppen der zweiten Ebene berücksichtigt.

Untergruppen von Gruppen mit nicht übereinstimmenden Kriterien werden nicht berücksichtigt. Eine Gruppe muss übereinstimmende Kriterien oder keine Kriterien besitzen, damit ihre Untergruppen für ein System berücksichtigt werden.

9 Auf diese Weise wird die Systemstruktur abwärts durchlaufen, bis ein System in eine Gruppe einsortiert ist.

Wenn die Server-Einstellung für die Systemstruktursortierung so konfiguriert ist, dass die Sortierung nur bei der ersten Agent-Server-Kommunikation erfolgt, wird das System entsprechend gekennzeichnet. Diese Kennzeichnung bedeutet, dass das System erst dann wieder bei einer Agent-Server-Kommunikation sortiert werden kann, wenn die Server-Einstellung so geändert wird, dass das Sortieren bei jeder Agent-Server-Kommunikation möglich ist.

10 Wenn der Server das System keiner Gruppe zuordnen kann, wird es in die Lost&Found-Gruppe in einer Untergruppe mit dem Namen seiner Domäne eingeordnet.

Erstellen und Auffüllen von Systemstrukturgruppen

Erstellen Sie Systemstrukturgruppen, und füllen Sie die Gruppen mit Systemen auf.

Außerdem können Sie ausgewählte Systeme in beliebige Gruppen in der Systemstruktur ziehen, um Gruppen aufzufüllen. Auf diese Weise können Sie Gruppen und Untergruppen auch innerhalb der Systemstruktur verschieben.

Es gibt viele verschiedene Möglichkeiten, eine Systemstruktur zu organisieren. Da sich jedes Netzwerk unterscheidet, kann die Organisation Ihrer Systemstruktur ebenso einmalig sein wie Ihr Netzwerklayout. Obwohl Sie nicht alle verfügbaren Methoden verwenden werden, können Sie mehrere einsetzen.

Wenn Sie zum Beispiel Active Directory in Ihrem Netzwerk verwenden, können Sie Ihre Active Directory-Container anstelle der NT-Domänen importieren. Wenn die Organisation der Active Directory- oder NT-Domänen für die Sicherheitsverwaltung nicht infrage kommt, können Sie die Organisation der Systemstruktur in einer Textdatei erstellen und sie dann in die Systemstruktur importieren. Wenn das Netzwerk kleiner ist, können Sie die Systemstruktur manuell erstellen und jedes System manuell hinzufügen.

Aufgaben

- *Manuelles Erstellen von Gruppen* auf Seite 123
  Erstellen Sie Untergruppen in der **Systemstruktur**. stattfindet.
- *Manuelles Hinzufügen von Systemen zu einer vorhandenen Gruppe* auf Seite 124
  Fügen Sie bestimmte Systeme zu einer ausgewählten Gruppe hinzu.
- *Exportieren von Systemen aus der Systemstruktur* auf Seite 124
  Sie können eine Liste von Systemen aus der Systemstruktur in eine TXT-Datei exportieren, um sie später zu verwenden. Der Export erfolgt auf Gruppen- oder Untergruppenebene unter Beibehaltung der Positionen in der Systemstruktur.
- *Importieren von Systemen aus einer Textdatei* auf Seite 125
  Sie können eine Textdatei mit einer Liste von Systemen und Gruppen für den Import in die Systemstruktur erstellen.
- *Sortieren von Systemen in kriterienbasierten Gruppen* auf Seite 126
  Sie können die Sortierung für die Gruppierung von Systemen konfigurieren und implementieren. Damit Systeme in Gruppen sortiert werden, muss die Sortierung aktiviert sein. Zudem müssen Sortierkriterien und die Sortierreihenfolge von Gruppen konfiguriert sein.
- *Importieren von Active Directory-Containern* auf Seite 129
  Sie können Systeme aus Active Directory-Containern direkt in die **Systemstruktur** importieren, indem Sie die Active Directory-Quellcontainer den **Systemstrukturgruppen** zuordnen.
- *Importieren von NT-Domänen in eine vorhandene Gruppe* auf Seite 130
  Sie können Systeme aus einer NT-Domäne in eine manuell erstellte Gruppe importieren.
- *Planen der Systemstruktursynchronisierung* auf Seite 132
  Sie können einen Server-Task planen, durch den die Systemstruktur mit Änderungen in der zugeordneten Domäne oder dem zugeordneten Active Directory-Container aktualisiert wird.
- *Manuelles Aktualisieren einer synchronisierten Gruppe mit einer NT-Domäne* auf Seite 133
  Aktualisieren Sie eine synchronisierte Gruppe mit Änderungen in der zugehörigen NT-Domäne.

Manuelles Erstellen von Gruppen

Erstellen Sie Untergruppen in der **Systemstruktur**. stattfindet.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Öffnen Sie das Dialogfeld Neue Untergruppen.

   a Wählen Sie die folgenden Optionen aus: **Menü** | **Systeme** | **Systemstruktur**.

   b Wählen Sie eine Gruppe aus.

   c Klicken Sie auf **Neue Untergruppen**.

   Sie können mehrere Untergruppen gleichzeitig erstellen.

2 Geben Sie einen Namen ein, und klicken Sie dann auf **OK**.

   Die neue Gruppe wird in der **Systemstruktur** angezeigt.

3 Wiederholen Sie diesen Schritt so oft, bis Sie die Gruppen mit den Systemen auffüllen können. Verwenden Sie eines der folgenden Verfahren, um Systeme zu den **Systemstrukturgruppen** hinzuzufügen:

- Manuelles Eingeben der Systemnamen.
- Importieren aus NT-Domänen oder Active Directory-Containern. Zur einfacheren Verwaltung können Sie eine Domäne oder einen Container regelmäßig mit einer Gruppe synchronisieren.
- Einrichten von IP-Adressen- oder Tag-basierten Sortierungskriterien für die Gruppen. Wenn Agenten von Systemen mit übereinstimmenden IP-Adressinformationen oder Tags einchecken, werden sie automatisch in die entsprechende Gruppe eingeordnet.

Manuelles Hinzufügen von Systemen zu einer vorhandenen Gruppe

Fügen Sie bestimmte Systeme zu einer ausgewählten Gruppe hinzu.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Öffnen Sie die Seite Neue Systeme.

a Wählen Sie die folgenden Optionen aus: **Menü** | **Systeme** | **Systemstruktur**.

b Klicken Sie auf **Neue Systeme**.

2 Wählen Sie aus, ob McAfee Agent auf den neuen Systemen bereitgestellt werden soll und ob die Systeme zur ausgewählten Gruppe oder entsprechend den Sortierungskriterien zu einer Gruppe hinzugefügt werden sollen.

3 Geben Sie neben **Zielsysteme** den NetBIOS-Namen für die einzelnen Systeme in das Textfeld ein, und trennen Sie diese mit Kommas, Leerzeichen oder Zeilenumbrüchen. Klicken Sie alternativ auf **Durchsuchen**, um die Systeme auszuwählen.

4 Geben Sie nach Bedarf weitere Optionen an.

Wenn Sie die Option **Agenten pushen und Systeme zur aktuellen Gruppe hinzufügen** ausgewählt haben, können Sie die automatische Sortierung der **Systemstruktur** aktivieren. Hiermit wenden Sie die Sortierungskriterien auf diese Systeme an.

5 Klicken Sie auf **OK**.

Exportieren von Systemen aus der Systemstruktur

Sie können eine Liste von Systemen aus der Systemstruktur in eine TXT-Datei exportieren, um sie später zu verwenden. Der Export erfolgt auf Gruppen- oder Untergruppenebene unter Beibehaltung der Positionen in der Systemstruktur.

Es kann nützlich sein, über eine Liste der Systeme aus der Systemstruktur zu verfügen. Sie können diese Liste in den McAfee ePO-Server importieren, um eine frühere Struktur und Anordnung schnell wiederherzustellen.

Die Systeme werden hierbei nicht aus der Systemstruktur entfernt. Es wird eine TXT-Datei erstellt, die die Namen und Struktur von Systemen in der Systemstruktur enthält.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur**. Die Seite **Systemstruktur** wird geöffnet.

2 Wählen Sie die Gruppe oder Untergruppe aus, in der sich die zu exportierenden Systeme befinden, und klicken Sie dann auf **Systemstrukturaktionen** | **Systeme exportieren**. Die Seite **Systeme exportieren** wird geöffnet.

3 Wählen Sie aus, welche Elemente exportiert werden sollen:

- **Allen Systemen in dieser Gruppe** – Exportiert die Systeme in der angegebenen **Quellgruppe**, jedoch keine Systeme, die sich in unterhalb dieser Ebene verschachtelten Untergruppen befinden.
- **Allen Systemen in dieser Gruppe und Untergruppen** – Exportiert alle auf und unterhalb dieser Ebene befindlichen Systeme.

4 Klicken Sie auf **OK**.

Die Seite **Exportieren** wird geöffnet. Sie können auf den Link **Systeme** klicken, um die Systemliste anzuzeigen, oder mit der rechten Maustaste auf den Link klicken, um eine Kopie der Datei **EXPORTSYSTEMS.TXT** zu speichern.

Importieren von Systemen aus einer Textdatei

Sie können eine Textdatei mit einer Liste von Systemen und Gruppen für den Import in die Systemstruktur erstellen.

Aufgaben

- *Erstellen einer Textdatei mit Gruppen und Systemen* auf Seite 125
  Sie können eine Textdatei mit den NetBIOS-Namen Ihrer Netzwerksysteme erstellen, die Sie in eine Gruppe importieren möchten. Dabei haben Sie die Möglichkeit, eine unsortierte Liste von Systemen zu importieren oder die Systeme in Gruppen zu unterteilen.
- *Importieren von Systemen und Gruppen aus einer Textdatei* auf Seite 126
  Sie können Systeme oder Systemgruppen aus einer Textdatei, die Sie erstellt und gespeichert haben, in die **Systemstruktur** importieren.

Erstellen einer Textdatei mit Gruppen und Systemen

Sie können eine Textdatei mit den NetBIOS-Namen Ihrer Netzwerksysteme erstellen, die Sie in eine Gruppe importieren möchten. Dabei haben Sie die Möglichkeit, eine unsortierte Liste von Systemen zu importieren oder die Systeme in Gruppen zu unterteilen.

Definieren Sie die Gruppen und deren Systeme, indem Sie die Gruppen- und Systemnamen in eine Textdatei eingeben. Importieren Sie diese Informationen dann in ePolicy Orchestrator. Bei größeren Netzwerken müssen Sie Netzwerkdienstprogramme verwenden (z. B. das im Microsoft Windows Resource Kit verfügbare Dienstprogramm Netdom.exe), um Textdateien mit vollständigen Listen der Systeme in Ihrem Netzwerk zu erstellen. Sobald die Textdatei erstellt ist, können Sie sie manuell bearbeiten, um Gruppen von Systemen zu erstellen und die gesamte Struktur in die Systemstruktur zu importieren.

Unabhängig davon, wie Sie die Textdatei erstellen, müssen Sie die richtige Syntax verwenden, bevor Sie sie importieren.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Jedes System muss auf einer separaten Zeile aufgeführt sein. Um die Systeme in Gruppen aufzuteilen, geben Sie den Gruppennamen gefolgt von einem umgekehrten Schrägstrich (\) ein. Führen Sie darunter die zugehörigen Systeme auf, wobei jedes System auf einer eigenen Zeile steht.

```
GruppeA\System1

GruppeA\System2

GruppeA\GruppeB\System3

GruppeC\GruppeD
```

2 Überprüfen Sie die Namen der Gruppen und Systeme sowie die Syntax der Textdatei. Speichern Sie anschließend die Textdatei in einem temporären Ordner auf dem Server.

Importieren von Systemen und Gruppen aus einer Textdatei

Sie können Systeme oder Systemgruppen aus einer Textdatei, die Sie erstellt und gespeichert haben, in die **Systemstruktur** importieren.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Öffnen Sie die Seite Neue Systeme.

a Wählen Sie die folgenden Optionen aus: **Menü** | **Systeme** | **Systemstruktur**.

b Klicken Sie auf **Neue Systeme**.

2 Wählen Sie **Systeme aus einer Textdatei in die ausgewählte Gruppe importieren, aber Agenten nicht pushen** aus.

3 Wählen Sie aus, ob die Importdatei folgende Elemente enthält:

- **Systeme und Systemstruktur**
- **Nur Systeme (als unsortierte Liste)**

4 Klicken Sie auf **Durchsuchen**, und wählen Sie die Textdatei aus.

5 Legen Sie fest, wie mit Systemen verfahren werden soll, die bereits an anderen Stellen in der **Systemstruktur** vorhanden sind.

6 Klicken Sie auf **OK**.

Die Systeme werden in die ausgewählte Gruppe in der **Systemstruktur** importiert. Wenn die Systeme in der Textdatei in Gruppen sortiert sind, werden diese Gruppen erstellt und die Systeme importiert.

Sortieren von Systemen in kriterienbasierten Gruppen

Sie können die Sortierung für die Gruppierung von Systemen konfigurieren und implementieren. Damit Systeme in Gruppen sortiert werden, muss die Sortierung aktiviert sein. Zudem müssen Sortierkriterien und die Sortierreihenfolge von Gruppen konfiguriert sein.

Aufgaben

- *Hinzufügen von Sortierungskriterien zu Gruppen* auf Seite 127
  Sortierungskriterien für Systemstrukturgruppen können auf IP-Adressinformationen oder Tags basieren.
- *Aktivieren der Systemstruktursortierung auf dem Server* auf Seite 127
  Die Systeme werden nur sortiert, wenn die Sortierung der Systemstruktur sowohl auf dem Server als auch auf den Systemen aktiviert ist.
- *Aktivieren oder Deaktivieren der Systemstruktursortierung auf Systemen* auf Seite 128
  Der Sortierungsstatus eines Systems bestimmt, ob es in eine kriterienbasierte Gruppe sortiert werden kann.
- *Manuelles Sortieren von Systemen* auf Seite 128
  Sie können ausgewählte Systeme mit aktivierter kriterienbasierter Sortierung in Gruppen sortieren.

Hinzufügen von Sortierungskriterien zu Gruppen

Sortierungskriterien für Systemstrukturgruppen können auf IP-Adressinformationen oder Tags basieren.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Gruppeninformationen**, und wählen Sie dann in der Systemstruktur die Gruppe aus.

2 Klicken Sie neben **Sortierungskriterien** auf **Bearbeiten**. Die Seite **Sortierungskriterien** für die ausgewählte Gruppe wird angezeigt.

3 Wählen Sie **Systeme, die mit einem der unten stehenden Sortierungskriterien übereinstimmen** aus. Die Kriterienauswahl wird angezeigt.

Obwohl Sie mehrere Sortierungskriterien für die Gruppe konfigurieren können, muss ein System nur ein einziges Kriterium erfüllen, um in diese Gruppe eingeordnet zu werden.

4 Konfigurieren Sie das Kriterium. Folgende Optionen stehen zur Auswahl:

- **IP-Adressen** – Definieren Sie in diesem Textfeld einen IP-Adressbereich oder eine IP-Subnetzmaske als Sortierungskriterium. Jedes System, dessen Adresse sich in diesem Bereich befindet, wird in diese Gruppe sortiert.
- **Tags** – Fügen Sie spezifische Tags hinzu, damit Systeme mit diesen Tags, die in die übergeordnete Gruppe eingeordnet werden, in diese Gruppe sortiert werden.

5 Wiederholen Sie diesen Vorgang so lange, bis die Sortierungskriterien für die Gruppe konfiguriert sind, und klicken Sie dann auf **Speichern**.

Aktivieren der Systemstruktursortierung auf dem Server

Die Systeme werden nur sortiert, wenn die Sortierung der Systemstruktur sowohl auf dem Server als auch auf den Systemen aktiviert ist.

Wenn Sie im folgenden Task festlegen, dass nur bei der ersten Agent-Server-Kommunikation sortiert werden soll, werden alle aktivierten Systeme bei ihrer nächsten Agent-Server-Kommunikation sortiert. Danach werden sie nicht mehr sortiert, solange diese Option ausgewählt ist. Sie können diese Systeme jedoch manuell erneut sortieren, indem Sie die Aktion **Jetzt sortieren** ausführen oder diese Einstellung so ändern, dass bei jeder Agent-Server-Kommunikation sortiert wird.

Wenn Sie festlegen, dass bei jeder Agent-Server-Kommunikation sortiert werden soll, werden alle aktivierten Systeme bei jeder Agent-Server-Kommunikation sortiert, solange diese Option ausgewählt ist.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste **Einstellungskategorien** den Eintrag **Systemstruktursortierung** aus, und klicken Sie dann auf **Bearbeiten**.
2. Legen Sie fest, ob Systeme nur bei der ersten oder bei jeder Agent-zu-Server-Kommunikation sortiert werden sollen.

Aktivieren oder Deaktivieren der Systemstruktursortierung auf Systemen

Der Sortierungsstatus eines Systems bestimmt, ob es in eine kriterienbasierte Gruppe sortiert werden kann.

Sie können den Sortierungsstatus auf Systemen in jeder beliebigen Tabelle mit Systemen (z. B. Abfrageergebnisse) sowie automatisch bei den Ergebnissen einer geplanten Abfrage ändern.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Systeme**, und wählen Sie dann die gewünschten Systeme aus.
2. Klicken Sie auf **Aktionen** | **Verzeichnisverwaltung** | **Sortierungsstatus ändern**, und wählen Sie dann aus, ob die Systemstruktursortierung auf ausgewählten Systemen aktiviert oder deaktiviert werden soll.
3. Wählen Sie im Dialogfeld Sortierungsstatus ändern aus, ob die Systemstruktursortierung auf dem ausgewählten System aktiviert oder deaktiviert werden soll.

Je nach der Einstellung für die Systemstruktursortierung werden diese Systeme bei der nächsten Agent-Server-Kommunikation sortiert. Andernfalls können sie nur mit der Aktion **Jetzt sortieren** sortiert werden.

Manuelles Sortieren von Systemen

Sie können ausgewählte Systeme mit aktivierter kriterienbasierter Sortierung in Gruppen sortieren.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Systeme**, und wählen Sie dann die Gruppe mit dem System aus.
2. Wählen Sie die Systeme aus, und klicken Sie dann auf **Aktionen** | **Verzeichnisverwaltung** | **Jetzt sortieren**. Das Dialogfeld Jetzt sortieren wird angezeigt.

Wenn Sie vor dem Sortieren eine Vorschau der Ergebnisse anzeigen möchten, klicken Sie auf **Sortiertest**. (Wenn Sie Systeme auf der Seite **Sortiertest** verschieben, werden jedoch alle ausgewählten Systeme sortiert, auch wenn die Systemstruktursortierung für sie deaktiviert ist.)

3. Klicken Sie auf **OK**, um die Systeme zu sortieren.

Importieren von Active Directory-Containern

Sie können Systeme aus Active Directory-Containern direkt in die **Systemstruktur** importieren, indem Sie die Active Directory-Quellcontainer den **Systemstrukturgruppen** zuordnen.

Durch Zuordnen von Active Directory-Containern zu Gruppen ist Folgendes möglich:

- Synchronisieren der **Systemstruktur** mit der Active Directory-Struktur, sodass beim Hinzufügen oder Entfernen von Containern in Active Directory die entsprechende Gruppe in der **Systemstruktur** ebenfalls hinzugefügt oder entfernt wird
- Löschen von Systemen in der **Systemstruktur**, wenn diese in Active Directory gelöscht werden
- Vermeiden von doppelten Systemeinträgen in der **Systemstruktur**, wenn die jeweiligen Systeme bereits in anderen Gruppen vorhanden sind

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Gruppeninformationen**, und wählen Sie dann in der **Systemstruktur** eine Gruppe aus, der Sie einen Active Directory-Container zuordnen möchten.

Die **Sammelgruppe** der **Systemstruktur** kann nicht synchronisiert werden.

2 Klicken Sie neben **Synchronisierungstyp** auf **Bearbeiten**. Die Seite **Synchronisierungseinstellungen** für die ausgewählte Gruppe wird angezeigt.

3 Klicken Sie neben **Synchronisierungstyp** auf **Active Directory**. Die Optionen für die Active Directory-Synchronisierung werden angezeigt.

4 Wählen Sie den Typ der Active Directory-Synchronisierung aus, die zwischen dieser Gruppe und dem Active Directory-Container (und seinen Untercontainern) stattfinden soll:

- **Systeme und Containerstruktur**: Wählen Sie diese Option aus, wenn diese Gruppe die Active Directory-Struktur vollständig widerspiegeln soll. Bei der Synchronisierung wird die **Systemstruktur** dieser Gruppe geändert, um die Struktur des Active Directory-Containers widerzuspiegeln, dem sie zugeordnet ist. Container, die in Active Directory hinzugefügt oder entfernt werden, werden auch in der **Systemstruktur** hinzugefügt bzw. entfernt. Systeme, die in Active Directory hinzugefügt, verschoben oder entfernt werden, werden auch der **Systemstruktur** hinzugefügt bzw. aus dieser verschoben oder entfernt.
- **Nur Systeme (als unsortierte Liste)** – Wählen Sie diese Option, wenn allein diese Gruppe ausschließlich mit Systemen aus dem Active Directory-Container (und nicht ausgeschlossenen Untercontainern) gefüllt werden soll. Beim Spiegeln von Active Directory werden keine Untergruppen erstellt.

5 Wählen Sie aus, ob Sie einen doppelten Eintrag für Systeme erstellen möchten, die in einer anderen Gruppe der **Systemstruktur** vorhanden sind.

Wenn Sie die Active Directory-Synchronisierung als Ausgangspunkt für die Sicherheitsverwaltung verwenden und nach der Zuordnung der Systeme die Verwaltungsfunktionen der **Systemstruktur** verwenden möchten, wählen Sie diese Option nicht aus.

6 Im Abschnitt **Active Directory-Domäne** haben Sie die folgenden Möglichkeiten:

- Geben Sie den vollqualifizierten Domänennamen der Active Directory-Domäne ein.
- Wählen Sie in einer Liste bereits registrierter LDAP-Server einen LDAP-Server aus.

7 Klicken Sie neben **Container** auf **Hinzufügen**. Wählen Sie im Dialogfeld **Active Directory-Container auswählen** einen Quellcontainer aus, und klicken Sie auf **OK**.

8 Klicken Sie zum Ausschließen bestimmter Untercontainer neben **Ausnahmen** auf **Hinzufügen**, und wählen Sie die auszuschließenden Untercontainer aus. Klicken Sie anschließend auf **OK**.

9 Wählen Sie aus, ob McAfee Agent automatisch auf neuen Systemen ausgebracht werden sollen. Wenn Sie diese Option auswählen, müssen Sie die Ausbringungseinstellungen konfigurieren.

McAfee Sie sollten McAfee Agent nicht während des Erstimports eines großen Containers ausbringen. Das gleichzeitige Ausbringen des 3,62 MB großen McAfee Agent-Pakets auf vielen Systemen kann zu einer Überlastung des Netzwerks führen. Stattdessen sollten Sie den Container importieren und McAfee Agent anschließend nicht auf allen Systemen gleichzeitig, sondern nacheinander in einzelnen Systemgruppen ausbringen. Sie sollten diese Seite erneut aufrufen und diese Option nach der ersten McAfee Agent-Ausbringung auswählen, damit McAfee Agent automatisch auf neu zu Active Directory hinzugefügten Systemen installiert wird.

10 Wählen Sie aus, ob Systeme beim Löschen in der Active Directory-Domäne auch in der **Systemstruktur** gelöscht werden sollen. Optional können Sie auswählen, ob Agenten von den gelöschten Systemen entfernt werden sollen.

11 Zum sofortigen Synchronisieren der Gruppe mit Active Directory klicken Sie auf **Jetzt synchronisieren**.

Wenn Sie auf **Jetzt synchronisieren** klicken, werden alle an den Synchronisierungseinstellungen vorgenommenen Änderungen vor dem Synchronisieren der Gruppe gespeichert. Wenn eine Benachrichtigungsregel für die Active Directory-Synchronisierung aktiviert ist, wird bei jedem hinzugefügten oder entfernten System ein Ereignis generiert. Diese Ereignisse werden im **Audit-Protokoll** angezeigt und können abgefragt werden. Wenn Sie Agenten auf hinzugefügten Systemen ausbringen, wird die Ausbringung für jedes hinzugefügte System ausgeführt. Nach Abschluss der Synchronisierung wird das Feld **Letzte Synchronisierung** aktualisiert. Dabei werden Uhrzeit und Datum der letzten Synchronisierung und nicht der abgeschlossenen Agenten-Ausbringungen angezeigt.

Sie können für die erste Synchronisierung einen Server-Task für die NT-Domänen-/Active Directory-Synchronisierung planen. Dieser Server-Task ist besonders dann nützlich, wenn Sie Agenten während der ersten Synchronisierung auf neuen Systemen ausbringen und die Bandbreite ein Problem darstellt.

12 Zeigen Sie nach Abschluss der Synchronisierung die Ergebnisse in der **Systemstruktur** an.

Bringen Sie nach dem Importieren der Systeme die Agenten auf ihnen aus, sofern Sie keine automatische Ausbringung ausgewählt haben.

Außerdem kann es sinnvoll sein, einen regelmäßigen Server-Task für die NT-Domänen-/Active Directory-Synchronisierung einzurichten, damit die **Systemstruktur** mit allen Änderungen in den Active Directory-Containern aktualisiert wird.

Importieren von NT-Domänen in eine vorhandene Gruppe

Sie können Systeme aus einer NT-Domäne in eine manuell erstellte Gruppe importieren.

Sie können Gruppen automatisch auffüllen, indem Sie ganze NT-Domänen mit bestimmten Gruppen synchronisieren. Mit dieser Vorgehensweise können Sie in einem Schritt sämtliche Systeme im Netzwerk als unsortierte Liste ohne Systembeschreibung der Systemstruktur hinzufügen.

Wenn die Domäne sehr groß ist, können Sie Untergruppen erstellen, um die Richtlinienverwaltung und die Organisation zu vereinfachen. Importieren Sie dazu zuerst die Domäne in eine Gruppe der Systemstruktur, und erstellen Sie dann manuell logische Untergruppen.

Importieren Sie zum Verwalten der gleichen Richtlinie in mehreren Domänen jede der Domänen in eine Untergruppe der gleichen Gruppe. Die Untergruppen erben die Richtlinien, die für die Gruppe der obersten Ebene festgelegt sind.

Beachten Sie bei dieser Vorgehensweise Folgendes:

- Legen Sie für Untergruppen IP-Adressen- oder Tag-basierte Sortierungskriterien fest, um die importierten Systeme automatisch zu sortieren.
- Planen Sie zur einfacheren Wartung einen regelmäßigen Server-Task für die NT-Domänen-/Active Directory-Synchronisierung.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Gruppeninformationen**, und wählen Sie in der **Systemstruktur** eine Gruppe aus, oder erstellen Sie eine neue Gruppe.

2 Klicken Sie neben **Synchronisierungstyp** auf **Bearbeiten**. Die Seite **Synchronisierungseinstellungen** für die ausgewählte Gruppe wird angezeigt.

3 Klicken Sie neben **Synchronisierungstyp** auf **NT-Domäne**. Die Einstellungen für die Domänensynchronisierung werden angezeigt.

4 Legen Sie neben **Systeme, die an anderen Stellen in der Systemstruktur vorhanden sind** fest, wie mit Systemen verfahren werden soll, die bereits in einer anderen Gruppe der **Systemstruktur** vorhanden sind.

Es wird nicht empfohlen, die Option **Systeme zur synchronisierten Gruppe hinzufügen und sie im aktuellen Speicherort in der Systemstruktur belassen** auszuwählen. Das gilt insbesondere dann, wenn Sie die NT-Domänensynchronisierung nur als Ausgangspunkt für die Sicherheitsverwaltung verwenden.

5 Klicken Sie neben **Domäne** auf **Durchsuchen**, und wählen Sie die NT-Domäne aus, die Sie dieser Gruppe zuordnen möchten. Klicken Sie dann auf **OK**. Alternativ können Sie den Namen der Domäne direkt in das Textfeld eingeben.

Geben Sie nicht den vollständigen Domänennamen ein.

6 Wählen Sie aus, ob McAfee Agent automatisch auf neuen Systemen ausgebracht werden sollen. Wenn Sie diese Option auswählen, müssen Sie die Ausbringungseinstellungen konfigurieren.

Sie sollten McAfee Agent nicht während des Erstimports einer großen Domäne ausbringen. Das gleichzeitige Ausbringen des 3,62 MB großen McAfee Agent-Pakets auf vielen Systemen kann zu einer Überlastung des Netzwerks führen. Stattdessen sollten Sie die Domäne importieren und den Agenten anschließend nicht auf allen Systemen gleichzeitig, sondern in kleineren Systemgruppen ausbringen. Wenn Sie McAfee Agent ausgebracht haben, können Sie zu dieser Seite zurückkehren und diese Option nach der ersten Agenten-Ausbringung auswählen. Auf diese Weise wird McAfee Agent automatisch auf neuen Systemen installiert, die der Gruppe (oder deren Untergruppen) durch die Domänensynchronisierung hinzugefügt werden.

7 Wählen Sie aus, ob Systeme beim Löschen in der NT-Domäne auch in der **Systemstruktur** gelöscht werden sollen. Optional können Sie auswählen, ob Agenten von den gelöschten Systemen entfernt werden sollen.

8 Zum sofortigen Synchronisieren der Gruppe mit der Domäne klicken Sie auf **Jetzt synchronisieren**, und warten Sie dann, bis die Systeme in der Domäne der Gruppe hinzugefügt wurden.

Wenn Sie auf **Jetzt synchronisieren** klicken, werden an den Synchronisierungseinstellungen vorgenommene Änderungen vor dem Synchronisieren der Gruppe gespeichert. Wenn eine Benachrichtigungsregel für die NT-Domänensynchronisierung aktiviert ist, wird bei jedem hinzugefügten oder entfernten System ein Ereignis generiert. Diese Ereignisse werden im **Audit-Protokoll** angezeigt und können abgefragt werden. Wenn Sie Agenten auf hinzugefügten Systemen ausbringen möchten, wird die Ausbringung für jedes hinzugefügte System ausgeführt. Nach Abschluss der Synchronisierung wird das Feld **Letzte Synchronisierung** aktualisiert. Dabei werden Uhrzeit und Datum der letzten Synchronisierung und nicht der abgeschlossenen Agenten-Ausbringungen angezeigt.

9 Klicken Sie zum manuellen Synchronisieren der Gruppe mit der Domäne auf **Vergleichen und aktualisieren**.

Durch Klicken auf **Vergleichen und aktualisieren** werden alle Änderungen an den Synchronisierungseinstellungen gespeichert.

a Wenn Sie über diese Seite Systeme aus der Gruppe entfernen, müssen Sie festlegen, ob deren Agenten beim Entfernen der Systeme ebenfalls entfernt werden sollen.

b Wählen Sie nach Bedarf die Systeme aus, die Sie der Gruppe hinzufügen bzw. daraus entfernen möchten. Klicken Sie dann auf **Gruppe aktualisieren**, um die ausgewählten Systeme hinzuzufügen. Die Seite **Synchronisierungseinstellungen** wird angezeigt.

10 Klicken Sie auf **Speichern**, und zeigen Sie dann die Ergebnisse in der **Systemstruktur** an, wenn Sie auf **Jetzt synchronisieren** oder **Gruppe aktualisieren** geklickt haben.

Bringen Sie nach dem Hinzufügen der Systeme zur **Systemstruktur** Agenten auf den Systemen aus, falls Sie nicht ausgewählt haben, dass Agenten im Rahmen der Synchronisierung ausgebracht werden sollen.

Außerdem kann es sinnvoll sein, einen regelmäßigen Server-Task für die NT-Domänen-/Active Directory-Synchronisierung einzurichten, damit diese Gruppe mit allen neuen Systemen in der NT-Domäne aktualisiert wird.

Planen der Systemstruktursynchronisierung

Sie können einen Server-Task planen, durch den die Systemstruktur mit Änderungen in der zugeordneten Domäne oder dem zugeordneten Active Directory-Container aktualisiert wird.

Je nach Synchronisierungseinstellungen der Gruppe werden mit diesem Task die folgenden Aktionen automatisiert:

- Hinzufügen neuer Systeme zur angegebenen Gruppe im Netzwerk
- Hinzufügen neuer zugehöriger Gruppen, wenn neue Active Directory-Container erstellt werden
- Löschen zugehöriger Gruppen, wenn Active Directory-Container entfernt werden
- Ausbringen von Agenten auf neue Systeme
- Entfernen von Systemen, die sich nicht mehr in der Domäne oder im Container befinden
- Anwenden von Richtlinien und Tasks für Sites oder Gruppen auf neue Systeme
- Verhindern oder Zulassen von Duplikaten für Systemeinträge, die noch in der Systemstruktur vorhanden sind, nachdem Sie sie an andere Stellen verschoben haben

McAfee Agent kann nicht auf allen Betriebssystemen auf diese Weise bereitgestellt werden. Möglicherweise müssen Sie McAfee Agent auf einigen Systemen manuell verteilen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Öffnen Sie den **Generator für Server-Tasks**.

   a Wählen Sie die folgenden Optionen aus: **Menü** | **Automatisierung** | **Server-Tasks**.

   b Klicken Sie auf **Neuer Task**.

2 Geben Sie auf der Seite Beschreibung einen Namen für den Task an, und wählen Sie aus, ob er nach dem Erstellen aktiviert werden soll. Klicken Sie dann auf **Weiter**.

3 Wählen Sie in der Dropdown-Liste den Eintrag **Active Directory-Synchronisierung/NT-Domäne** aus.

4 Wählen Sie aus, ob alle oder nur ausgewählte Gruppen synchronisiert werden sollen. Wenn Sie nur einige Gruppen synchronisieren möchten, klicken Sie auf **Synchronisierte Gruppen auswählen**, und wählen Sie die gewünschten Gruppen aus.

5 Klicken Sie auf **Weiter**, um die Seite Plan zu öffnen.

6 Planen Sie den Task, und klicken Sie dann auf **Weiter**.

7 Überprüfen Sie die Task-Details, und klicken Sie dann auf **Speichern**.

Sie können den Task nicht nur zum geplanten Zeitpunkt, sondern auch sofort ausführen: Klicken Sie auf der Seite Server-Tasks neben dem Task auf **Ausführen**.

Manuelles Aktualisieren einer synchronisierten Gruppe mit einer NT-Domäne

Aktualisieren Sie eine synchronisierte Gruppe mit Änderungen in der zugehörigen NT-Domäne.

Die Aktualisierung beinhaltet die folgenden Änderungen:

- Hinzufügen von Systemen, die aktuell in der Domäne vorhanden sind
- Entfernen von Systemen aus der Systemstruktur, die sich nicht mehr in der Domäne befinden
- Entfernen von Agenten aus allen Systemen, die nicht mehr zur angegebenen Domäne gehören

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Gruppeninformationen**, und wählen Sie dann die Gruppe aus, die der NT-Domäne zugewiesen ist.

2 Klicken Sie neben **Synchronisierungstyp** auf **Bearbeiten**. Die Seite **Synchronisierungseinstellungen** wird angezeigt.

3 Wählen Sie **NT-Domäne** aus, und klicken Sie dann unten auf der Seite auf **Vergleichen und aktualisieren**. Die Seite **Manuell vergleichen und aktualisieren** wird angezeigt.

4 Legen Sie beim Entfernen von Systemen aus der Gruppe fest, ob die Agenten von entfernten Systemen ebenfalls entfernt werden sollen.

5 Klicken Sie auf **Alle hinzufügen** bzw. **Hinzufügen**, um Systeme aus der Netzwerkdomäne in die ausgewählte Gruppe zu importieren.

   Klicken Sie auf **Alle entfernen** bzw. **Entfernen**, um Systeme aus der ausgewählten Gruppe zu entfernen.

6 Klicken Sie abschließend auf **Gruppe aktualisieren**.

Verschieben von Systemen innerhalb der Systemstruktur

Verschieben Sie Systeme aus einer Gruppe in der Systemstruktur in eine andere. Sie können Systeme von beliebigen Seiten verschieben, auf denen eine Tabelle mit Systemen (einschließlich der Ergebnisse einer Abfrage) angezeigt wird.

Zusätzlich zu den unten angegebenen Schritten können Sie Systeme auch aus der Tabelle **Systeme** in eine beliebige Systemstrukturgruppe ziehen und dort ablegen.

Selbst wenn Sie Ihre Systemstruktur so gut organisiert haben, dass sie Ihre Netzwerkhierarchie genau wiedergibt, und Sie die Systemstruktur regelmäßig mithilfe automatisierter Tasks und Tools synchronisieren, müssen Sie möglicherweise Systeme manuell zwischen Gruppen verschieben. Beispielsweise könnte es erforderlich sein, dass Sie Systeme in bestimmten Abständen aus der Sammelgruppe verschieben müssen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Systeme**, suchen Sie die Systeme, und wählen Sie sie aus.
2. Klicken Sie auf **Aktionen** | **Verzeichnisverwaltung** | **Systeme verschieben**. Die Seite **Neue Gruppe auswählen** wird angezeigt.
3. Legen Sie fest, ob die Systemstruktursortierung auf den ausgewählten Systemen beim Verschieben aktiviert oder deaktiviert werden soll.
4. Wählen Sie die Gruppe aus, in die die Systeme eingeordnet werden sollen, und klicken Sie dann auf **OK**.

Funktionsweise von Systeme übertragen

Mit dem Befehl Systeme übertragen können Sie verwaltete Systeme zwischen registrierten McAfee ePO-Servern verschieben.

Möglicherweise müssen Sie diese verwalteten Systeme übertragen, wenn Sie die Server-Hardware und das Betriebssystem oder die Server-Hardware und die Software-Version von McAfee ePO aktualisieren.

In diesem Diagramm sehen Sie die wichtigsten Prozesse, die zum Übertragen von Systemen zwischen McAfee ePO-Servern erforderlich sind.

Zum Übertragen verwalteter Systeme zwischen McAfee ePO-Servern gehören die oben in der Abbildung gezeigten sechs Prozesse.

1. **ASSC-Schlüssel (Schlüssel für sichere Agenten-Server-Kommunikation) exportieren**: Verwenden Sie auf dem alten McAfee ePO-Server die Optionen **Menü** | **Server-Einstellungen** | **Sicherheitsschlüssel**.
2. **ASSC-Schlüssel importieren**: Verwenden Sie auf dem neuen McAfee ePO-Server die Optionen **Menü** | **Server-Einstellungen** | **Sicherheitsschlüssel**.
3. **Sekundären McAfee ePO-Server registrieren**: Verwenden Sie auf dem alten McAfee ePO-Server die Optionen **Menü** | **Konfiguration** | **Registrierte Server**.
4. **Systeme auf den sekundären McAfee ePO-Server verschieben**: Verwenden Sie auf dem alten McAfee ePO-Server die Optionen **Menü** | **Systemstruktur** | **Systeme** (Registerkarte) und **Aktionen** | **Agent** | **Systeme übertragen**.

5 **Eintreffen der Systeme überprüfen**: Verwenden Sie auf dem neuen McAfee ePO-Server die Optionen **Menü** | **Systemstruktur** | **Systeme** (Registerkarte).

6 **Verschieben der Systeme überprüfen**: Verwenden Sie auf dem alten McAfee ePO-Server die Optionen **Menü** | **Systemstruktur** | **Systeme** (Registerkarte).

Siehe auch

Exportieren und Importieren von ASSC-Schlüsseln zwischen McAfee ePO-Servern auf Seite 136
Registrieren von McAfee ePO-Servern auf Seite 91
Übertragen von Systemen zwischen McAfee ePO-Servern auf Seite 135

Übertragen von Systemen zwischen McAfee ePO-Servern

Mit Systeme übertragen können Sie verwaltete Systeme zwischen registrierten McAfee ePO-Servern verschieben.

Bevor Sie beginnen

Damit Sie verwaltete Systeme zwischen zwei McAfee ePO-Servern verschieben können, beispielsweise zwischen einem alten und einem neuen McAfee ePO-Server, müssen Sie an beiden McAfee ePO-Konfigurationen die folgenden Änderungen vornehmen:

Die folgenden Schritte bewirken eine bidirektionale Übertragung. Wenn Sie nur eine unidirektionale Übertragung aktivieren möchten, ist es nicht notwendig, die ASSC-Schlüssel (Schlüssel für sichere Agenten-Server-Kommunikation) des neuen McAfee ePO-Servers auf dem alten McAfee ePO-Server zu importieren.

- Verknüpfen Sie die Schlüssel für sichere Agenten-Server-Kommunikation zwischen den beiden McAfee ePO-Servern.
  1 Exportieren Sie die ASSC-Schlüssel von beiden Servern.
  2 Importieren Sie die ASSC-Schlüssel des alten Servers auf dem neuen Server.
  3 Importieren Sie die ASSC-Schlüssel des neuen Servers auf dem alten Server.
- Registrieren Sie den alten und den neuen McAfee ePO-Server, damit Sie die Systeme hin- und herübertragen können.

  Aktivieren Sie unbedingt Systeme übertragen, und wählen Sie auf der Seite Details der Seite Generator für registrierte Server die Option Automatischer Sitelist-Import aus.

Die Schritte in diesem Task beschreiben das Übertragen von Systemen von einem alten McAfee ePO-Server auf einen neuen Server.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf dem alten McAfee ePO-Server auf **Menü** | **Systeme** | **Systemstruktur**, und wählen Sie dann die zu übertragenden Systeme aus.

2 Klicken Sie auf **Aktionen** | **Agent** | **Systeme übertragen**.

3 Wählen Sie im Dialogfeld Systeme übertragen im Dropdown-Menü den neuen McAfee ePO-Server aus, und klicken Sie auf **OK**.

Nachdem ein verwaltetes System zur Übertragung gekennzeichnet wurde, müssen zwei Agent-Server-Kommunikationsintervalle auftreten, bevor das System in der Systemstruktur des Ziel-Servers angezeigt wird. Wie lange es dauert, bis diese beiden Kommunikationsintervalle abgeschlossen sind, hängt von der Konfiguration ab. Das standardmäßige Agent-Server-Kommunikationsintervall beträgt eine Stunde.

Siehe auch

Funktionsweise von Systeme übertragen auf Seite 134
Exportieren und Importieren von ASSC-Schlüsseln zwischen McAfee ePO-Servern auf Seite 136
Registrieren von McAfee ePO-Servern auf Seite 91

Exportieren und Importieren von ASSC-Schlüsseln zwischen McAfee ePO-Servern

Damit Sie Systeme zwischen McAfee ePO-Servern übertragen können, müssen Sie die ASSC-Schlüssel (Schlüssel für sichere Agenten-Server-Kommunikation) zwischen den McAfee ePO-Servern exportieren und importieren.

Mithilfe von Schlüsseln für sichere Agenten-Server-Kommunikation können Agenten sicher mit dem McAfee ePO-Server kommunizieren. Wenn Sie ein verwaltetes System mit einer verschlüsselten McAfee Agent-Version auf einen anderen McAfee ePO-Server übertragen, ohne die zugehörigen Client-Schlüssel zu importieren, kann auf dem übertragenen System keine Verbindung mit dem neuen McAfee ePO-Server hergestellt werden.

Zum Übertragen verwalteter Systeme in beide Richtungen müssen Sie die beiden Server gegenseitig registrieren und beide ASSC-Schlüsselsätze exportieren und importieren.

Wenn Sie einen McAfee ePO-Server zu registrieren versuchen und die Option **Systeme übertragen** mit dem automatischen Sitelist-Import aktivieren, bevor Sie die ASSC-Schlüssel zwischen den McAfee ePO-Servern exportieren und importieren, wird die folgende Fehlermeldung angezeigt:

FEHLER: Die Agent-Server-Hauptschlüssel müssen vor dem Importieren der Sitelist in den Remote-Server importiert werden. Rufen Sie die Server-Einstellungen auf, um Sicherheitsschlüssel von diesem Server zu exportieren. Wenn Sie jetzt auf diesen Link klicken, gehen alle nicht gespeicherten Änderungen an diesem registrierten Server verloren.

Sie müssen die 1024-Bit- und die 2048-Bit-Versionen der ASSC-Schlüssel vom McAfee ePO-Server importieren, um die Automatische Sitelist zu registrieren und zu importieren.

Mit den folgenden Schritten exportieren und importieren Sie die ASSC-Schlüssel von einem McAfee ePO-Server auf einen anderen.

In diesen Schritten wird das Exportieren der ASSC-Schlüssel von einem *alten* McAfee ePO-Server auf einen *neuen* McAfee ePO-Server beschrieben.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf dem alten McAfee ePO-Server auf **Menü** | **Konfiguration** | **Server-Einstellungen**. Klicken Sie in der Spalte **Einstellungskategorien** auf **Sicherheitsschlüssel**, und klicken Sie dann auf **Bearbeiten**.

Führen Sie zum Exportieren der beiden ASSC-Schlüssel die folgenden Schritte aus:

a Zum Exportieren des 2.048-Bit-ASSC-Schlüssels wählen Sie auf der Seite Sicherheitsschlüssel: Bearbeiten in der Liste Schlüssel für sichere Agenten-Server-Kommunikation den 2.048-Bit-Schlüssel aus. Klicken Sie auf **Exportieren** und dann im Dialogfeld Schlüssel für sichere Agenten-Server-Kommunikation exportieren auf **OK**.

b Speichern Sie die ZIP-Datei in einem temporären Ordner auf dem lokalen Computer.

Der Standardname der Datei mit dem 2.048-Bit-ASSC-Schlüssel lautet sr2048<Server-Name>.zip, wobei <Server-Name> der Name des McAfee ePO-Servers ist. So entspricht beispielsweise im Dateinamen sr2048ePO50_server.zip die Zeichenfolge "ePO50_server" dem Server-Namen.

c Zum Exportieren des 1.024-Bit-ASSC-Schlüssels wählen Sie auf der Seite Sicherheitsschlüssel: Bearbeiten in der Liste der Schlüssel für sichere Agenten-Server-Kommunikation den 1.024-Bit-Schlüssel aus. Klicken Sie auf **Exportieren** und dann im Dialogfeld Schlüssel für sichere Agenten-Server-Kommunikation exportieren auf **OK**. Speichern Sie die ZIP-Datei im gleichen temporären Ordner auf dem lokalen Computer.

2 Klicken Sie auf dem neuen McAfee ePO-Server auf **Menü** | **Konfiguration** | **Server-Einstellungen**. Klicken Sie in der Spalte **Einstellungskategorien** auf **Sicherheitsschlüssel**, und klicken Sie dann auf **Bearbeiten**.

Führen Sie zum Importieren der beiden ASSC-Schlüssel die folgenden Schritte aus:

a Klicken Sie auf der Seite Sicherheitsschlüssel: Bearbeiten neben der Gruppe Schlüssel importieren und sichern auf **Importieren**.

b Navigieren Sie auf der Seite Schlüssel importieren zu dem Speicherort, an dem Sie die ZIP-Dateien der in Schritt 1 exportierten 2.048-Bit- und 1.024-Bit-ASSC-Schlüssel gespeichert haben.

c Wählen Sie im Dialogfeld **Datei zum Hochladen auswählen** die ZIP-Datei mit dem 2.048-Bit-ASSC-Schlüssel aus. Daraufhin wird wieder die Seite Schlüssel importieren angezeigt. Klicken Sie auf **Weiter**.

d Vergewissern Sie sich auf der Seite Übersicht, dass Sie den richtigen Schlüssel ausgewählt haben, und klicken Sie auf **Speichern**.

e Zum Importieren des 1.024-Bit-ASSC-Schlüssels führen Sie erneut die Schritte a bis d aus.

3 Vergewissern Sie sich auf dem neuen McAfee ePO-Server, dass sowohl der 1.024-Bit- als auch der 2.048-Bit-ASSC-Schlüssel in der Liste Schlüssel für sichere Agenten-Server-Kommunikation aufgeführt ist. Klicken Sie dann auf **Speichern**.

Beide ASSC-Schlüssel sind jetzt auf dem neuen McAfee ePO-Server gespeichert, und Sie können den neuen McAfee ePO-Server erfolgreich beim alten Server registrieren. Anschließend können Sie mit Systeme übertragen die verwalteten Systeme verschieben.

Zusammenspiel der Funktion für automatische Antworten mit der Systemstruktur

Bevor Sie mit dem Planen der Implementierung von automatischen Antworten beginnen, sollten Sie genau verstehen, wie diese Funktion im Zusammenhang mit der Systemstruktur arbeitet.

Diese Funktion hält nicht das beim Erzwingen von Richtlinien verwendete Vererbungsmodell ein.

Automatische Antworten verwenden Ereignisse, die auf Systemen in der Umgebung auftreten, die an den Server übermittelt werden und Antwortregeln ausgelöst haben, die der Gruppe mit den betroffenen Systemen und den übergeordneten Elementen zugeordnet sind. Wenn die Bedingungen einer dieser Regeln erfüllt sind, werden gemäß der Konfiguration der Regel vorher festgelegte Aktionen ausgeführt.

Auf diese Weise können Sie unabhängige Regeln auf unterschiedlichen Ebenen der Systemstruktur konfigurieren. Folgende Eigenschaften können sich für diese Regeln unterscheiden:

- **Schwellenwerte für das Senden einer Benachrichtigung**. So möchte zum Beispiel ein Administrator einer bestimmten Gruppe benachrichtigt werden, wenn innerhalb von 10 Minuten auf 100 Systemen in der Gruppe Viren entdeckt werden, ein anderer Administrator jedoch erst, wenn dies im selben Zeitraum in der gesamten Umgebung auf mindestens 1.000 Systemen geschieht.
- **Empfänger der Benachrichtigung**. Ein Administrator einer bestimmten Gruppe möchte beispielsweise nur dann eine Benachrichtigung erhalten, wenn eine bestimmte Anzahl von Virusentdeckungen in der Gruppe auftritt. Oder ein Administrator möchte, dass alle Gruppenadministratoren eine Benachrichtigung erhalten, wenn eine bestimmte Anzahl von Virusentdeckungen in der gesamten Systemstruktur auftritt.

Server-Ereignisse werden nicht nach dem Speicherort in der Systemstruktur gefiltert.

Beschränkung, Aggregation und Gruppierung

Durch Festlegen von Schwellenwerten, die auf Aggregation, Beschränkung und Gruppierung basieren, können Sie konfigurieren, wann Benachrichtigungen gesendet werden.

Aggregation

Mit der Aggregation können Sie Schwellenwerte für Ereignisse festlegen, ab denen die Regel eine Benachrichtigung sendet. Konfigurieren Sie eine Regel zum Beispiel so, dass eine Benachrichtigung gesendet wird, wenn der Server innerhalb einer Stunde 1.000 Virusentdeckungen von unterschiedlichen Systemen oder 100 Virusentdeckungen von einem System empfängt.

Beschränkung

Wenn Sie eine Regel konfiguriert haben, nach der Sie bei einem möglichen Virenausbruch benachrichtigt werden, können Sie mit der Beschränkung sicherstellen, dass Sie nicht zu viele Benachrichtigungen erhalten. Als Administrator eines umfangreichen Netzwerks erhalten Sie möglicherweise Zehntausende Ereignisse innerhalb einer Stunde, was bei einer solchen Regel zu Tausenden von Benachrichtigungen führen würde. Mithilfe von Antworten können Sie die Anzahl der Benachrichtigungen beschränken, die Sie aufgrund einer einzelnen Regel erhalten. Sie können beispielsweise in derselben Regel bestimmen, dass Sie lediglich eine Benachrichtigung pro Stunde erhalten möchten.

Gruppierung

Mittels Gruppierung können Sie mehrere aggregierte Ereignisse zusammenfassen. So können zum Beispiel Ereignisse mit dem gleichen Schweregrad in einer einzigen Gruppe zusammengefasst werden. Durch eine Gruppierung kann der Administrator auf alle Ereignisse mit diesem oder einem höheren Schweregrad gleichzeitig reagieren. Außerdem können Sie damit auch für die bei verwalteten Systemen oder Servern generierten Ereignisse Prioritäten vergeben.

Standardregeln

Aktivieren Sie die ePolicy Orchestrator-Standardregeln, um die Funktion zum Ausprobieren sofort verwenden zu können.

Vor dem Aktivieren von Standardregeln sollten Sie die folgenden Schritte ausführen:

- Geben Sie den E-Mail-Server an (unter **Menü** | **Konfiguration** | **Server-Einstellungen**), von dem die Benachrichtigungsmeldungen gesendet werden.
- Vergewissern Sie sich, dass Sie die E-Mail-Adresse der Person angeben, die E-Mail-Benachrichtigungen empfangen soll. Diese Adresse wird im Assistenten auf der Seite **Aktionen** festgelegt.

Tabelle 9-1 Standardbenachrichtigungsregeln

Regelname	Zugehörige Ereignisse	Konfigurationen
Fehler beim Aktualisieren oder Replizieren des verteilten Repositorys	Fehler beim Aktualisieren oder Replizieren des verteilten Repositorys	Sendet eine Benachrichtigung, wenn bei einer Aktualisierung oder einer Replizierung ein Fehler auftritt.
Malware entdeckt	Ereignisse von unbekannten Produkten	Sendet eine Benachrichtigung: • Die Anzahl der Ereignisse erreicht innerhalb einer Stunde mindestens den Wert 1.000. • Eine Benachrichtigung wird max. alle zwei Stunden gesendet. • Sofern vorhanden und zusammen mit vielen anderen Parametern werden die IP-Adresse des Quellsystems, die Bezeichnung für die aktuelle Bedrohung und Informationen zum aktuellen Produkt mitgesendet. • Die Anzahl ausgewählter eindeutiger Werte beträgt 500.
Fehler beim Aktualisieren oder Replizieren des Master-Repositorys	Fehler beim Aktualisieren oder Replizieren des Master-Repositorys	Sendet eine Benachrichtigung, wenn bei einer Aktualisierung oder einer Replizierung ein Fehler auftritt.
Nicht konformer Computer entdeckt	Ereignisse vom Typ Nicht konformer Computer entdeckt	Sendet eine Benachrichtigung, wenn ein Ereignis vom Server-Task Compliance-Ereignis generieren empfangen wird.

10 Tags

Setzen Sie Tags ein, um Systeme zu identifizieren und zu sortieren. Über Tags und Tag-Gruppen können Sie Systemgruppen auswählen und das Erstellen von Tasks und Abfragen vereinfachen.

Inhalt

- *Erstellen von Tags mit dem Tag-Generator*
- *Tags verwalten*
- *Erstellen, Löschen und Ändern von Tag-Untergruppen*
- *Ausschließen von Systemen von der automatischen Kennzeichnung*
- *Erstellen einer Abfrage zum Auflisten von Systemen anhand der Tags*
- *Anwenden von Tags auf ausgewählte Systeme*
- *Löschen eines Tags vom System*
- *Anwenden von kriterienbasierten Tags auf alle übereinstimmenden Systeme*
- *Planmäßiges Anwenden von kriterienbasierten Tags*

Erstellen von Tags mit dem Tag-Generator

Mit dem Tag-Generator können Sie Tags schnell erstellen.

Tags können Kriterien verwenden, auf die hin jedes System bewertet wird:

- Automatisch bei der Agent-zu-Server-Kommunikation.
- Wenn die Aktion **Tag-Kriterien ausführen** ausgeführt wird.
- Manuell auf ausgewählten Systemen mit der Aktion **Tag anwenden**, unabhängig von den Kriterien.

Tags ohne Kriterien können nur manuell auf ausgewählte Systeme angewendet werden.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Öffnen Sie den **Tag-Generator**: Klicken Sie auf **Menü** | **Systeme** | **Tag-Katalog** | **Neues Tag**.
2. Geben Sie auf der Seite **Beschreibung** einen Namen und eine eindeutige Beschreibung ein, und klicken Sie anschließend auf **Weiter**. Die Seite **Kriterien** wird angezeigt.
3. Wählen Sie die Kriterien aus, und konfigurieren Sie diese. Klicken Sie anschließend auf **Weiter**. Die Seite **Test** wird angezeigt.

Wenn das Tag automatisch angewendet werden soll, müssen Sie Kriterien für das Tag konfigurieren.

4 Legen Sie fest, ob Systeme nur bei der Aktion **Tag-Kriterien ausführen** oder auch bei jeder Agent-Server-Kommunikation anhand der Tag-Kriterien bewertet werden sollen. Klicken Sie anschließend auf **Weiter**. Die Seite **Vorschau** wird angezeigt.

Diese Optionen sind nur verfügbar, wenn Kriterien konfiguriert wurden. Beim Bewerten von Systemen anhand von Tag-Kriterien wird das Tag auf Systeme angewendet, die die Kriterien erfüllen und nicht von diesem Tag ausgeschlossen wurden.

5 Überprüfen Sie die Informationen auf dieser Seite, und klicken Sie dann auf **Speichern**.

Wenn das Tag über Kriterien verfügt, wird auf dieser Seite die Anzahl an Systemen angezeigt, die dieses Tag beim Bewerten anhand der Tag-Kriterien erhalten.

Das Tag wird auf der Seite **Tag-Katalog** in der **Tag-Struktur** unter der ausgewählten Tag-Gruppe hinzugefügt.

Tags verwalten

Die mit dem Tag-Generator erstellten Tags können Sie mit der Liste Aktionen bearbeiten, löschen und verschieben.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Systeme** | **Tag-Katalog**.

2 Wählen Sie in der Liste **Tags** mindestens ein Tag aus, klicken Sie auf **Aktionen**, und wählen Sie in der Liste eine der folgenden Aktionen aus.

Aktion	Schritte
Bearbeiten eines Tags Die Anzahl der betroffenen Systeme wird oben auf der Seite angezeigt.	Gehen Sie in **Bearbeiten – Tag-Generator** wie folgt vor: **1** Geben Sie auf der Seite **Beschreibung** einen Namen und eine eindeutige Beschreibung ein, und klicken Sie anschließend auf **Weiter**. Die Seite **Kriterien** wird angezeigt. **2** Wählen Sie die Kriterien aus, und konfigurieren Sie diese. Klicken Sie anschließend auf **Weiter**. Die Seite **Test** wird angezeigt. Wenn das Tag automatisch angewendet werden soll, müssen Sie Kriterien für das Tag konfigurieren. **3** Legen Sie fest, ob Systeme nur bei der Aktion **Tag-Kriterien ausführen** oder auch bei jeder Agent-Server-Kommunikation anhand der Tag-Kriterien bewertet werden sollen. Klicken Sie anschließend auf **Weiter**. Die Seite **Vorschau** wird angezeigt. Diese Optionen sind nur verfügbar, wenn Kriterien konfiguriert wurden. Beim Bewerten von Systemen anhand von Tag-Kriterien wird das Tag auf Systeme angewendet, die die Kriterien erfüllen und nicht von diesem Tag ausgeschlossen wurden. **4** Überprüfen Sie die Informationen auf dieser Seite, und klicken Sie dann auf **Speichern**. Wenn das Tag über Kriterien verfügt, wird auf dieser Seite die Anzahl der Systeme angezeigt, die dieses Tag beim Bewerten anhand der Tag-Kriterien erhalten. Das Tag wird auf der Seite **Tag-Katalog** in der **Tag-Struktur** unter der ausgewählten Tag-Gruppe aktualisiert.
Löschen eines Tags	Klicken Sie auf **Löschen**. Das Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf **OK**, um das Tag zu löschen.
Exportieren eines Tags	Klicken Sie auf **Tabelle exportieren**. Die Seite **Daten exportieren** wird angezeigt.
Tags verschieben	Gehen Sie im Dialogfeld **Tags verschieben** wie folgt vor: **1** Wählen Sie die Tag-Gruppe aus, in der die Tags angezeigt werden sollen. **2** Klicken Sie auf **OK**, um das Verschieben abzuschließen. Sie können die Tags auch in die Tag-Gruppen in der **Tag-Struktur** ziehen und dort ablegen.

Erstellen, Löschen und Ändern von Tag-Untergruppen

Mithilfe von Tag-Untergruppen können Sie Tag-Gruppen vier Ebenen tief verschachteln, wobei jede übergeordnete Gruppe bis zu 1.000 Tag-Untergruppen enthalten kann. Mit diesen Tag-Gruppen und kriterienbasierter Sortierung können Sie Systeme automatisch den richtigen Gruppen hinzufügen.

Mit den folgenden Schritten können Sie eine Tag-Untergruppe erstellen, löschen oder ändern.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Systeme** | **Tag-Katalog**.

2 Wählen Sie auf der Seite **Tag-Katalog** eine der folgenden Aktionen aus.

Aktion	Schritte
Erstellen einer Tag-Untergruppe	1 Wählen Sie in der hierarchischen Liste **Tag-Struktur** die Tag-Gruppe (oder die übergeordnete Tag-Gruppe) aus, in der Sie die neue Tag-Untergruppe erstellen möchten. **Meine Tags** wird bei der Installation von ePolicy Orchestrator als standardmäßige Tag-Gruppe der obersten Ebene hinzugefügt. 2 Klicken Sie auf **Neue Untergruppe**, um das Dialogfeld **Neue Untergruppe** anzuzeigen. 3 Geben Sie im Feld **Name** einen aussagekräftigen Namen für die neue Tag-Untergruppe ein. 4 Klicken Sie abschließend auf **OK**, um die neue Tag-Untergruppe zu erstellen.
Umbenennen einer Tag-Untergruppe	1 Wählen Sie in der hierarchischen Liste **Tag-Struktur** die Tag-Untergruppe aus, die Sie umbenennen möchten. 2 Klicken Sie auf **Tag-Struktur-Aktionen**	**Gruppe umbenennen**, um das Dialogfeld **Untergruppe umbenennen** anzuzeigen. 3 Geben Sie im Feld **Name** den neuen Namen für die Tag-Untergruppe ein. 4 Klicken Sie abschließend auf **OK**. Die Tag-Untergruppe wird daraufhin umbenannt.
Löschen einer Tag-Untergruppe	1 Wählen Sie in der hierarchischen Liste **Tag-Struktur** die Tag-Untergruppe aus, die Sie löschen möchten. 2 Klicken Sie auf **Aktionen**	**Löschen**. Daraufhin wird das Bestätigungsdialogfeld **Aktion: Löschen** angezeigt. 3 Wenn Sie sicher sind, dass Sie die Tag-Untergruppe löschen möchten, klicken Sie auf **OK**. Die Tag-Untergruppe wird daraufhin entfernt.

Ausschließen von Systemen von der automatischen Kennzeichnung

Sie können Systeme von der Anwendung bestimmter Tags ausschließen.

Wahlweise können Sie Systeme auch mit einer Abfrage erfassen und die gewünschten Tags dann mithilfe der Abfrageergebnisse von diesen Systemen ausschließen.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Systeme**, und wählen Sie dann in der **Systemstruktur** die Gruppe aus, die die Systeme enthält.

2 Wählen Sie in der Tabelle **Systeme** mindestens ein System aus, und klicken Sie dann auf **Aktionen** | **Tag** | **Tag ausschließen**.

3 Wählen Sie im Dialogfeld **Tag ausschließen** die Tag-Gruppe sowie das auszuschließende Tag aus, und klicken Sie dann auf **OK**.

Um die Liste auf bestimmte Tags zu beschränken, geben Sie den Tagnamen in das Textfeld unter **Tags** ein.

4 Überprüfen Sie die Systeme, die vom Tag ausgeschlossen wurden:

a Öffnen Sie die Seite **Tag-Details**: Klicken Sie auf **Menü** | **Systeme** | **Tag-Katalog**, und wählen Sie dann das Tag oder die Tag-Gruppe in der Tag-Liste aus.

b Klicken Sie neben **Systeme mit Tag** auf den Link, um die Anzahl der von der kriterienbasierten Tag-Anwendung ausgeschlossenen Systeme zu erhalten. Die Seite **Vom Tag ausgeschlossene Systeme** wird angezeigt.

c Vergewissern Sie sich, dass sich die Systeme in der Liste befinden.

Erstellen einer Abfrage zum Auflisten von Systemen anhand der Tags

Planen Sie eine Abfrage, um eine Liste zu erstellen, über die ausgewählte Tags auf den entsprechenden Systemen angezeigt, übernommen oder entfernt werden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Öffnen Sie den **Generator für Server-Tasks**.

a Wählen Sie die folgenden Optionen aus: **Menü** | **Automatisierung** | **Server-Tasks**.

b Klicken Sie auf **Neuer Task**.

2 Geben Sie auf der Seite Beschreibung einen Namen und eine Beschreibung für den Task ein, und klicken Sie dann auf **Weiter**.

3 Wählen Sie im Dropdown-Menü **Aktionen** den Eintrag **Abfrage ausführen** aus.

4 Wählen Sie im Feld **Abfrage** eine der folgenden Abfragen auf der Registerkarte **McAfee-Gruppen** aus, und klicken Sie dann auf **OK**.

- **Inaktive Agenten**
- **Doppelte Systemnamen**
- **Systeme mit vielen Sequenzfehlern**
- **Systeme ohne neue Reihenfolgefehler**
- **Nicht verwaltete Systeme**

5 Wählen Sie die Sprache aus, in der die Ergebnisse angezeigt werden sollen.

6 Wählen Sie in der Liste **Unteraktionen** eine dieser Unteraktionen aus, die basierend auf den Ergebnissen ausgeführt werden soll.

- **Tag anwenden**: Auf alle in den Abfrageergebnissen enthaltenen Systeme wird ein bestimmtes Tag angewendet.
- **Tag löschen**: Ein ausgewähltes Tag wird auf allen in den Abfrageergebnissen enthaltenen Systemen entfernt. Wählen Sie **Alle löschen** aus, um alle Tags für die in den Abfrageergebnissen enthaltenen Systeme zu entfernen.
- **Tag ausschließen**: Schließt Systeme mit dem ausgewählten Tag aus den Abfrageergebnissen aus.

7 Wählen Sie im Fenster **Tag auswählen** eine Tag-Gruppe aus der **Tag-Gruppenstruktur** aus, und filtern Sie optional die Liste der Tags mithilfe des Textfelds **Tags**.

Sie können auch mehrere Aktionen für die Abfrageergebnisse auswählen. Klicken Sie auf die Schaltfläche **+**, um weitere Aktionen hinzuzufügen, die für die Abfrageergebnisse ausgeführt werden sollen. Achten Sie dabei darauf, die Aktionen in der Reihenfolge anzuordnen, in der sie für die Abfrageergebnisse ausgeführt werden sollen. Sie können beispielsweise das Tag Server anwenden und dann das Tag Workstation entfernen. Außerdem können Sie weitere Unteraktionen hinzufügen, beispielsweise zum Zuweisen einer Richtlinie zu den Systemen.

8 Klicken Sie auf **Weiter**.

9 Planen Sie den Task, und klicken Sie dann auf **Weiter**.

10 Überprüfen Sie die Konfiguration des Tasks, und klicken Sie dann auf **Speichern**.

Der Task wird zur Liste auf der Seite Server-Tasks hinzugefügt. Wenn der Task aktiviert ist (Standardeinstellung), wird er zum nächsten geplanten Zeitpunkt ausgeführt. Ein deaktivierter Task nur dann ausgeführt, wenn Sie auf der Seite **Server-Tasks** neben dem Task auf Ausführen klicken.

Anwenden von Tags auf ausgewählte Systeme

Sie können ein Tag manuell auf ausgewählte Systeme in der Systemstruktur anwenden.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Systeme**, und wählen Sie dann die Gruppe mit dem gewünschten System aus.

2 Wählen Sie die Systeme aus, und klicken Sie dann auf **Aktionen** | **Tag** | **Tag anwenden**.

3 Wählen Sie im Dialogfeld **Tag anwenden** die Tag-Gruppe sowie das anzuwendende Tag aus, und klicken Sie dann auf **OK**.

Um die Liste auf bestimmte Tags zu beschränken, geben Sie den Tagnamen in das Textfeld unter **Tags** ein.

4 Überprüfen Sie, ob die Tags angewendet wurden:

a Klicken Sie auf **Menü** | **Systeme** | **Tag-Katalog**, und wählen Sie dann in der Tag-Liste ein Tag oder eine Tag-Gruppe aus.

b Klicken Sie im Detailbereich neben **Systeme mit Tag** auf den Link, um die Anzahl der manuell gekennzeichneten Systeme zu erhalten. Die Seite **Systeme mit manuell angewendetem Tag** wird angezeigt.

c Vergewissern Sie sich, dass sich die Systeme in der Liste befinden.

Löschen eines Tags vom System

Entfernen Sie Tags von ausgewählten Systemen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Systeme**, und wählen Sie dann die Gruppe mit dem gewünschten System aus.
2. Wählen Sie die Systeme aus, und klicken Sie dann auf **Aktionen** | **Tag** | **Tag löschen**.
3. Führen Sie im Dialogfeld **Tag löschen** einen dieser Schritte durch, und klicken Sie anschließend auf **OK**.
   - Bestimmtes Tag entfernen: Wählen Sie die Tag-Gruppe und anschließend das Tag aus.

     Um die Liste auf bestimmte Tags zu beschränken, geben Sie den Tagnamen in das Textfeld unter **Tags** ein.
   - Alle Tags entfernen: Wählen Sie **Alle löschen** aus.
4. Überprüfen Sie, ob die Tags angewendet wurden:
   a. Klicken Sie auf **Menü** | **Systeme** | **Tag-Katalog**, und wählen Sie dann in der Tag-Liste ein Tag oder eine Tag-Gruppe aus.
   b. Klicken Sie im Detailbereich neben **Systeme mit Tag** auf den Link, um die Anzahl der manuell gekennzeichneten Systeme zu erhalten. Die Seite **Systeme mit manuell angewendetem Tag** wird angezeigt.
   c. Vergewissern Sie sich, dass sich die Systeme in der Liste befinden.

Anwenden von kriterienbasierten Tags auf alle übereinstimmenden Systeme

Sie können ein kriterienbasiertes Tag auf alle nicht ausgeschlossenen Systeme anwenden, die mit den angegebenen Kriterien übereinstimmen.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Systeme** | **Tag-Katalog**, und wählen Sie dann ein Tag oder eine Tag-Gruppe in der Liste **Tags** aus.
2. Klicken Sie auf **Aktionen** | **Tag-Kriterien ausführen**.
3. Wählen Sie im Bereich **Aktion** aus, ob Sie manuell gekennzeichnete oder ausgeschlossene Systeme zurücksetzen möchten.

   Beim Zurücksetzen manuell gekennzeichneter und ausgeschlossener Systeme wird das Tag von Systemen entfernt, die nicht mit den Kriterien übereinstimmen, während das Tag auf die Systeme angewendet wird, die mit den Kriterien übereinstimmen, aber vom Erhalt des Tags ausgeschlossen wurden.
4. Klicken Sie auf **OK**.

5 Überprüfen Sie, ob das Tag auf die Systeme angewendet wurde:

   a Klicken Sie auf **Menü** | **Systeme** | **Tag-Katalog**, und wählen Sie dann in der Tag-Liste ein Tag oder eine Tag-Gruppe aus.

   b Klicken Sie im Detailbereich neben **Systeme mit Tag** auf den Link, um die Anzahl der Systeme mit nach Kriterien angewendeten Tags zu erhalten. Die Seite **Systeme mit nach Kriterien angewendetem Tag** wird angezeigt.

   c Vergewissern Sie sich, dass sich die Systeme in der Liste befinden.

Das Tag wird auf alle Systeme angewendet, die seine Kriterien erfüllen.

Planmäßiges Anwenden von kriterienbasierten Tags

Sie können einen regelmäßigen Task planen, der ein Tag auf alle Systeme anwendet, die die Tag-Kriterien erfüllen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Öffnen Sie den **Generator für Server-Tasks**.

   a Wählen Sie die folgenden Optionen aus: **Menü** | **Automatisierung** | **Server-Tasks**.

   b Klicken Sie auf **Neuer Task**.

2 Geben Sie auf der Seite Beschreibung einen Namen und eine Beschreibung für den Task ein, wählen Sie aus, ob der Task bei der Erstellung aktiviert wird, und klicken Sie dann auf **Weiter**. Die Seite Aktionen wird angezeigt.

3 Wählen Sie in der Dropdown-Liste die Option **Tag-Kriterien ausführen** aus, und wählen Sie anschließend in der Dropdown-Liste **Tag** ein Tag aus.

4 Legen Sie fest, ob manuell gekennzeichnete oder ausgeschlossene Systeme zurückgesetzt werden sollen.

   Das Zurücksetzen manuell gekennzeichneter und ausgeschlossener Systeme hat zwei Auswirkungen:

   - Das Tag wird von Systemen entfernt, die nicht den Kriterien entsprechen.
   - Das Tag wird auf Systeme angewendet, die den Kriterien entsprechen, aber vom Erhalt des Tags ausgeschlossen wurden.

5 Klicken Sie auf **Weiter**, um die Seite Plan zu öffnen.

6 Planen Sie den Task für die gewünschten Zeiten ein, und klicken Sie dann auf **Weiter**.

7 Überprüfen Sie die Task-Einstellungen, und klicken Sie dann auf **Speichern**.

Der Server-Task wird zur Liste auf der Seite Server-Tasks hinzugefügt. Wenn Sie den Task im Assistenten Generator für Server-Tasks aktiviert haben, wird er zum nächsten geplanten Zeitpunkt ausgeführt.

11 Agent-zu-Server-Kommunikation

Für Client-Systeme wird McAfee Agent zur Kommunikation mit Ihrem McAfee ePO-Server verwendet. Überwachen und verwalten Sie Agenten über die ePolicy Orchestrator-Konsole.

Versionsspezifische Informationen zu den Agenten finden Sie im *McAfee Agent-Produkthandbuch*.

Inhalt

- *Arbeiten mit dem Agenten auf dem McAfee ePO-Server*
- *Verwalten der Agenten-Server-Kommunikation*

Arbeiten mit dem Agenten auf dem McAfee ePO-Server

Die McAfee ePO-Benutzeroberfläche verfügt über Seiten, auf denen Sie Agenten-Tasks und Richtlinien konfigurieren sowie Systemeigenschaften, Agenten-Eigenschaften und sonstige McAfee-Produktinformationen anzeigen können.

Inhalt

- *Funktionsweise der Agent-zu-Server-Kommunikation*
- *SuperAgents und ihre Funktionsweise*
- *McAfee Agent-Relay-Funktionalität*
- *Peer-to-Peer-Kommunikation*
- *Erfassen von McAfee Agent-Statistiken*
- *Ändern der in der Benutzeroberfläche und dem Ereignisprotokoll des Agenten verwendeten Sprache*
- *Konfigurieren von ausgewählten Systemen für die Aktualisierung*
- *Antworten auf Richtlinienereignisse*
- *Planen von Client-Tasks*
- *Sofortiges Ausführen von Client-Tasks*
- *Ermitteln inaktiver Agenten*
- *Windows-Systeme und vom Agenten gemeldete Produkteigenschaften*
- *Von McAfee Agent bereitgestellte Abfragen*

Funktionsweise der Agent-zu-Server-Kommunikation

Zwischen McAfee Agent und dem McAfee ePO-Server findet regelmäßig eine Kommunikation statt, um Ereignisse zu senden und sicherzustellen, dass alle Einstellungen aktuell sind.

Diese Kommunikationsvorgänge werden als *Agent-Server-Kommunikation* bezeichnet. Bei jeder Agent-Server-Kommunikation werden für McAfee Agent aktuelle Systemeigenschaften sowie alle noch nicht gesendeten Ereignisse erfasst und an den Server gesendet. Neue oder geänderte Richtlinien und Tasks sowie die Repository-Liste, falls sich diese seit der letzten Agent-Server-Kommunikation geändert hat, werden über den Server an McAfee Agent gesendet. Die neuen Richtlinien werden mit McAfee Agent lokal auf den verwalteten Systemen erzwungen, Task- oder Repository-Änderungen werden angewendet.

Für den McAfee ePO-Server wird ein branchenübliches, standardisiertes TLS-Netzwerkprotokoll (Transport Layer Security) für sichere Netzwerkübertragungen verwendet.

Wenn McAfee Agent erstmals installiert wird, wird innerhalb einiger Sekunden eine Verbindung zum Server hergestellt. Danach wird erneut eine Verbindung zwischen McAfee Agent und Server hergestellt, wenn eine der folgenden Situationen eintritt:

- Das Agent-Server-Kommunikationsintervall (ASKI) ist abgelaufen.
- McAfee Agent-Reaktivierungsaufrufe werden vom McAfee ePO-Server oder von Agenten-Handlern gesendet.
- Wenn ein geplanter Reaktivierungs-Task auf den Client-Systemen ausgeführt wird.
- Die Kommunikation wird manuell vom verwalteten System initiiert (über den Agent-Statusmonitor oder die Befehlszeile).
- McAfee Agent-Reaktivierungsaufrufe werden vom McAfee ePO-Server gesendet.

Agent-zu-Server-Kommunikationsintervall

Mit dem Agent-zu-Server-Kommunikationsintervall (ASKI) wird bestimmt, wie oft mit McAfee Agent eine Verbindung mit dem McAfee ePO-Server hergestellt wird.

Das Agent-zu-Server-Kommunikationsintervall wird auf der McAfee Agent-Richtlinienseite der Registerkarte **Allgemein** festgelegt. Die Standardeinstellung von 60 Minuten bedeutet, dass der McAfee ePO-Server einmal pro Stunde durch McAfee Agent kontaktiert wird. Wenn Sie über eine Intervalländerung nachdenken, sollten Sie beachten, dass in jedem ASKI die folgenden Aktionen durch McAfee Agent durchgeführt werden:

- Er erfasst und sendet seine Eigenschaften.
- Er sendet Ereignisse von niedriger Priorität, die seit der letzten Agent-zu-Server-Kommunikation aufgetreten sind.
- Neue Richtlinien und Tasks werden erhalten. Durch diese Aktion wird möglicherweise eine andere ressourcenintensive Aktion ausgelöst, die auf empfangenen Tasks und/oder Plänen basiert.
- Er erzwingt Richtlinien.

Auch wenn diese Aktivitäten einen einzelnen Computer nicht belasten, kann eine Reihe von Faktoren dazu führen, dass die Lasten im Netzwerk, auf McAfee ePO-Servern oder in Agenten-Handlern deutlich ansteigen. Das wäre zum Beispiel unter den folgenden Umständen der Fall:

- Wie viele Systeme über den McAfee ePO-Server verwaltet werden
- Hat Ihr Unternehmen verbindliche Anforderungen an die Reaktion auf Bedrohungen?
- Ist das Netzwerk oder der Standort der Clients im Bezug auf Server oder Agentensteuerungen stark verteilt?
- Ist die verfügbare Bandbreite nicht ausreichend?

Wenn diese Punkte auf Ihre Umgebung zutreffen, sollten Agent-Server-Kommunikationsvorgänge weniger oft durchgeführt werden. Für einzelne Clients mit wichtigen Funktionen können Sie ein kürzeres Intervall festlegen.

Behandeln von Unterbrechungen bei der Agent-zu-Server-Kommunikation

Bei der Behandlung von Kommunikationsunterbrechungen werden Probleme behoben, die verhindern, dass ein System eine Verbindung zu einem McAfee ePO-Server herstellen kann.

Unterbrechungen der Kommunikation können aus vielerlei Gründen auftreten. Der Algorithmus für die Agent-zu-Server-Kommunikation ist so ausgelegt, dass ein erneuter Versuch durchgeführt wird, wenn der erste Verbindungsversuch fehlschlägt.

Es wird versucht, mit McAfee Agent über eine dieser Methoden eine Verbindung herzustellen. Wenn alle Methoden fehlschlagen, wird während der nächsten Agent-zu-Server-Kommunikation ein erneuter Versuch von McAfee Agent vorgenommen, eine Verbindung herzustellen.

- IP-Adresse
- Vollqualifizierter Domänenname
- NetBIOS-Name

Reaktivierungen und Reaktivierungs-Tasks

Ein McAfee Agent-Reaktivierungsaufruf löst sofort und nicht erst nach Ablauf des aktuellen Agent-Server-Kommunikationsintervalls eine Agent-Server-Kommunikation aus.

Verwenden Sie Aktionen der **Systemstruktur**, um McAfee Agent unter Nicht-Windows-Betriebssystemen zu reaktivieren.

Eine Reaktivierung kann auf zwei Arten ausgegeben werden:

- **Manuell auf dem Server**: Das ist die gebräuchlichste Methode. Hierbei ist erforderlich, dass der Kommunikationsport für McAfee Agent-Reaktivierungen geöffnet ist.
- **Nach einem vom Administrator festgelegten Zeitplan**: Diese Methode ist nützlich, wenn die manuelle Agent-Server-Kommunikation laut Richtlinie deaktiviert ist. Der Administrator kann einen Reaktivierungs-*Task* erstellen und bereitstellen, mit dem McAfee Agent reaktiviert und die Agent-Server-Kommunikation initiiert wird.

Für die Ausgabe eines Reaktivierungsaufrufs gibt es u. a. folgende Gründe:

- Sie haben an einer Richtlinie eine Änderung vorgenommen, die unverzüglich und nicht erst nach Ablauf des nächsten geplanten Agent-zu-Server-Kommunikationsintervalls erzwungen werden soll.
- Sie haben einen neuen Task erstellt, der sofort ausgeführt werden soll. Mit der Option **Client-Task jetzt ausführen** wird ein Task erstellt, der dann den angegebenen Client-Systemen zugewiesen wird und mit dem Reaktivierungsaufrufe gesendet werden.
- Von einer Abfrage wurde ein Bericht generiert, aus dem hervorgeht, dass ein Client nicht konform ist, und Sie möchten nun dessen Status im Rahmen einer Fehlerbehebung testen.

Wenn Sie einen bestimmten McAfee Agent in einen **SuperAgent** konvertiert haben, können Sie über diesen Reaktivierungsaufrufe an vorgegebene Übertragungssegmente im Netzwerk senden. Durch **SuperAgents** wird die Bandbreitenauswirkung von Reaktivierungsaufrufen verteilt.

Senden manueller Reaktivierungen an einzelne Systeme

Das manuelle Senden einer Agenten- oder SuperAgent-Reaktivierung an Systeme in der **Systemstruktur** ist nützlich, wenn Sie Richtlinien ändern und möchten, dass sich Agenten schon vor der nächsten Agent-zu-Server-Kommunikation melden, um die aktualisierten Informationen zu senden oder zu empfangen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur**, und wählen Sie dann die Gruppe aus, in der sich die Zielsysteme befinden.

2 Wählen Sie in der Liste die Systeme aus, und klicken Sie dann auf **Aktionen** | **Agent** | **Agenten reaktivieren**.

3 Vergewissern Sie sich, dass die von Ihnen ausgewählten Systeme im Abschnitt **Zielsysteme** angezeigt werden.

4 Legen Sie neben **Reaktivierungstyp** fest, ob eine **Agenten-Reaktivierung** oder eine **SuperAgent-Reaktivierung** gesendet werden soll.

5 Übernehmen Sie den Standardwert (0 Minuten), oder geben Sie ein anderes Intervall für den **Zufallsgenerator** ein (0 – 60 Minuten). Beachten Sie dabei, wie viele Systeme die Reaktivierung sofort empfangen würden und wie viel Bandbreite verfügbar ist. Wenn Sie 0 eingeben, reagieren die Agenten sofort.

6 Damit bei dieser Reaktivierung inkrementelle Produkteigenschaften gesendet werden, müssen Sie die Option **Zusätzlich zu Systemeigenschaften vollständige Produkteigenschaften abrufen** deaktivieren. In der Standardeinstellung werden vollständige Produkteigenschaften gesendet.

7 Damit bei dieser Reaktivierung alle Richtlinien und Tasks aktualisiert werden, aktivieren Sie die Option **Vollständige Richtlinien- und Task-Aktualisierung erzwingen**.

8 Geben Sie bei **Anzahl der Versuche**, **Wiederholungsintervall** und **Abbrechen nach** eigene Werte für diese Reaktivierung ein, falls Sie die Standardeinstellungen nicht übernehmen möchten.

9 Wählen Sie aus, ob die Agenten-Reaktivierung über **Alle Agentensteuerungen** oder über die **Zuletzt verbundene Agentensteuerung** erfolgen soll.

10 Klicken Sie auf **OK**, um die Agenten- oder SuperAgent-Reaktivierung zu senden.

Senden manueller Reaktivierungen an eine Gruppe

Eine Agent- oder SuperAgent-Reaktivierung kann in einer einzigen Aufgabe an eine ganze **Systemstruktur**-Gruppe gesendet werden. Dies ist nützlich, wenn Sie Richtlinien geändert haben und möchten, dass sich Agenten schon vor der nächsten Agent-zu-Server-Kommunikation melden, um die aktualisierten Informationen zu senden oder zu empfangen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur**.

2 Wählen Sie in der **Systemstruktur** die Zielgruppe aus, und klicken Sie dann auf die Registerkarte **Gruppeninformationen**.

3 Klicken Sie auf **Aktionen** | **Agenten reaktivieren**.

4 Vergewissern Sie sich, dass neben **Zielgruppe** die ausgewählte Gruppe angezeigt wird.

5 Wählen Sie aus, ob eine Agenten-Reaktivierung zu **Allen Systemen in dieser Gruppe** oder **Allen Systemen in dieser Gruppe und Untergruppen** gesendet werden soll.

6 Legen Sie neben **Typ** fest, ob eine **Agenten-Reaktivierung** oder eine **SuperAgent-Reaktivierung** gesendet werden soll.

7 Übernehmen Sie den Standardwert (0 Minuten), oder geben Sie ein anderes Intervall für den **Zufallsgenerator** ein (0 – 60 Minuten). Wenn Sie `0` eingeben, reagieren die Agenten sofort.

8 Damit bei dieser Reaktivierung minimale Produkteigenschaften gesendet werden, deaktivieren Sie die Option **Zusätzlich zu Systemeigenschaften vollständige Produkteigenschaften abrufen**. In der Standardeinstellung werden vollständige Produkteigenschaften gesendet.

9 Damit bei dieser Reaktivierung alle Richtlinien und Tasks aktualisiert werden, aktivieren Sie die Option **Vollständige Richtlinien- und Task-Aktualisierung erzwingen**.

10 Klicken Sie auf **OK**, um die Agenten- oder SuperAgent-Reaktivierung zu senden.

SuperAgents und ihre Funktionsweise

Ein SuperAgent ist ein verteiltes Repository, dessen Inhaltsreplikation vom McAfee ePO-Server verwaltet wird.

Die von einem McAfee ePO-Server, dem Master-Repository, einem HTTP- oder einem FTP-Repository empfangenen Informationen werden vom SuperAgent im Cache abgelegt und an die Agenten in der Übertragungsdomäne verteilt. Sie sollten in jeder Übertragungsdomäne einen **SuperAgent** konfigurieren, wenn Sie Agenten in größeren Netzwerken verwalten.

Die Funktion für verzögertes Caching ermöglicht es, dass für einen SuperAgent Daten von McAfee ePO-Servern nur auf Anfrage von einem lokalen Agentenknoten abgerufen werden. Durch die Erstellung einer SuperAgent-Hierarchie zusammen mit verzögertem Caching können Sie weiter Bandbreite einsparen und die Last auf dem McAfee ePO-Server minimieren. Zum Aktivieren dieses Verhaltens klicken Sie auf der Seite mit den Richtlinienoptionen für **McAfee Agent** | **SuperAgent**, die Sie über **Menü** | **Richtlinie** | **Richtlinienkatalog** erreichen, auf **Verzögertes Caching aktivieren**.

Von einem SuperAgent werden auch Reaktivierungsaufrufe an andere Agenten gesendet, die sich im gleichen Netzwerksubnetz befinden. Der SuperAgent empfängt einen Reaktivierungsaufruf vom McAfee ePO-Server und reaktiviert dann die Agenten in seinem Subnetz.

Dies ist eine Alternative zum Senden gewöhnlicher Aufrufe zur Agentenreaktivierung an jeden Agenten im Netzwerk oder zum Senden von Agentenreaktivierungs-Tasks an jeden Computer.

SuperAgents und Übertragung von Reaktivierungsaufrufen

Verwenden Sie Reaktivierungsaufrufe, um die Agent-Server-Kommunikation zu initiieren, und ziehen Sie die Konvertierung von McAfee Agent in jeder Übertragungsdomäne in einen **SuperAgent** in Betracht.

Durch **SuperAgents** wird die Bandbreitenbelastung bei gleichzeitig ausgeführten Reaktivierungsaufrufen verteilt. Anstatt Reaktivierungsaufrufe vom Server an McAfee Agent zu senden, werden die **SuperAgent**-Reaktivierungsaufrufe vom Server an **SuperAgents** im ausgewählten Systemstruktursegment gesendet.

Der Prozess läuft folgendermaßen ab:

1 Der Reaktivierungsaufruf wird vom Server an alle **SuperAgents** gesendet.

2 Ein Reaktivierungsaufruf wird über die **SuperAgents** an McAfee Agent in derselben Übertragungsdomäne übertragen.

3 Über alle benachrichtigten McAfee Agent (von einem **SuperAgent** benachrichtigter McAfee Agent und alle **SuperAgents**) werden Daten mit dem McAfee ePO-Server oder Agenten-Handler ausgetauscht.

Wenn ein **SuperAgent**-Reaktivierungsaufruf gesendet wird, wird McAfee Agent ohne aktiven **SuperAgent** in der Übertragungsdomäne nicht zur Kommunikation mit dem Server aufgefordert.

Tipps für die Bereitstellung von SuperAgents

Um genügend **SuperAgents** an den richtigen Speicherorten bereitzustellen, bestimmen Sie zunächst die Übertragungsdomänen in Ihrer Umgebung. Wählen Sie anschließend in jeder Domäne ein System (vorzugsweise einen Server) aus, das als **SuperAgent**-Host dienen soll. Wenn Sie **SuperAgents** verwenden, stellen Sie sicher, dass McAfee Agent immer ein **SuperAgent** zugewiesen ist.

Für McAfee Agent- und **SuperAgent**-Reaktivierungsaufrufe werden dieselben sicheren Kanäle verwendet. Vergewissern Sie sich, dass die folgenden Ports nicht von einer Firewall auf dem Client blockiert werden:

- Der Kommunikationsport für McAfee Agent-Reaktivierungsaufrufe (standardmäßig Port 8081).
- Der Kommunikationsport für die McAfee Agent-Übertragung (standardmäßig Port 8082).

Konvertieren von McAfee Agent in einen SuperAgent

Wenn während der globalen Aktualisierung eine Aktualisierung vom McAfee ePO-Server an den **SuperAgent** gesendet wird, werden Reaktivierungsaufrufe an alle McAfee Agent im Netzwerk gesendet. Konfigurieren Sie **SuperAgent**-Richtlinieneinstellungen, um McAfee Agent in einen **SuperAgent** zu konvertieren.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Systeme**, und wählen Sie dann in der Systemstruktur eine Gruppe aus. Alle Systeme aus dieser Gruppe werden im Detailbereich angezeigt.
2. Wählen Sie ein System aus, und klicken Sie auf **Aktionen** | **Agent** | **Richtlinien auf einem einzelnen System ändern**. Die Seite Richtlinienzuweisung für dieses System wird angezeigt.
3. Wählen Sie in der Dropdown-Liste mit den Produkten den Eintrag **McAfee Agent** aus. Die Richtlinienkategorien unter **McAfee Agent** werden mit der dem System zugewiesenen Richtlinie aufgeführt.
4. Wenn die Richtlinie geerbt wurde, aktivieren Sie die Option **Vererbung unterbrechen und ab hier Richtlinie und Einstellungen zuweisen**.
5. Wählen Sie in der Dropdown-Liste **Zugewiesene Richtlinie** eine Richtlinie vom Typ **Allgemein** aus.

   Von diesem Speicherort können Sie die ausgewählte Richtlinie bearbeiten oder eine Richtlinie erstellen.

6. Legen Sie fest, ob die Richtlinienvererbung gesperrt werden soll, um zu verhindern, dass Systemen, die diese Richtlinie erben, eine andere Richtlinie zugewiesen wird.
7. Wählen Sie auf der Registerkarte **SuperAgent** die Option **Agenten in SuperAgents konvertieren** aus, um die Übertragung von Reaktivierungen zu ermöglichen.
8. Klicken Sie auf **Speichern**.
9. Senden Sie eine Agenten-Reaktivierung.

Caching und Kommunikationsunterbrechungen bei SuperAgents

Mit dem SuperAgent werden die Repository-Inhalte auf eine bestimmte Weise im Cache gespeichert, die darauf ausgelegt ist, die Last auf dem McAfee ePO-Server zu minimieren.

Wenn ein Agent in einen SuperAgent umgewandelt wurde, können über ihn vom McAfee ePO-Server, von verteilten Repositories oder von anderen SuperAgents bezogene Inhalte im Cache abgelegt werden, um sie lokal an andere Agenten zu verteilen. Dadurch wird die Last auf dem McAfee ePO-Server reduziert.

- SuperAgent-Caching sollte nicht zusammen mit Repository-Replizierungen verwendet werden.
- Inhalte aus HTTP- oder -FTP-Repositories von McAfee können von den SuperAgents nicht im Cache abgelegt werden.

Funktionsweise des Caches

Wenn Inhalte erstmals von einem Client-System angefordert werden, werden angeforderte Inhalte aus den konfigurierten Repositories über die diesem System zugewiesenen SuperAgents heruntergeladen und im Cache gespeichert. Der Cache wird jedes Mal aktualisiert, wenn eine neuere Version des angeforderten Pakets im Master-Repository zur Verfügung steht. In einer hierarchischen Struktur von SuperAgents erhält ein untergeordneter SuperAgent die angeforderten Inhaltsaktualisierungen aus dem Cache des ihm übergeordneten SuperAgents.

Vom SuperAgent werden definitiv nur solche Inhalte zwischengespeichert, die von den ihm zugewiesenen Agenten benötigt werden, da Inhalte immer erst auf Anfrage eines Clients aus den Repositories abgerufen werden. Dadurch wird der Datenverkehr zwischen dem SuperAgent und den Repositories minimiert. Während des Abrufs der Inhalte aus dem Repository durch den SuperAgent werden Anfragen von Client-Systemen für diese Inhalte angehalten.

Der SuperAgent muss über Zugriff auf das Repository verfügen. Ohne diesen Zugriff würden Agenten, die Aktualisierungen vom SuperAgent beziehen, neue Inhalte nie erhalten. Stellen Sie sicher, dass die SuperAgent-Richtlinie den Zugriff auf das Repository einschließt.

Agenten, die für die Verwendung des SuperAgents als Repository konfiguriert sind, erhalten die Inhalte aus dem Cache des SuperAgents anstatt direkt vom McAfee ePO-Server. Dies verbessert die Leistung des Agentensystems, da der überwiegende Teil des Netzwerkverkehrs für den SuperAgent und dessen Clients lokal erfolgt.

Wenn Sie den SuperAgent so umkonfigurieren, dass ein neues Repository verwendet wird, wird der Cache in Bezug auf das neue Repository aktualisiert.

Wann die Inhalte des verzögerten Caches bereinigt werden

Sie können den SuperAgent so konfigurieren, dass nicht verwendete Cache-Inhalte bereinigt werden. Der Cache-Inhalt wird heruntergeladen, wenn von einem Client-System eine Aktualisierung angefordert wird. Die vorherigen Aktualisierungsdateien sind möglicherweise noch auf dem lokalen Datenträger verfügbar, sind aber nicht in der Datei `Replica.log` aufgelistet. Wenn eine Datei nicht in `Replica.log` aufgelistet ist, wird sie bereinigt, da sie von keinem Client-System angefordert wird.

Die Datei `Replica.log` enthält Informationen zu Dateien und Ordnern im entsprechenden Verzeichnis. Jedes Verzeichnis im Repository enthält eine `Replica.log`-Datei.

Standardmäßig werden die Cache-Inhalte jeden Tag bereinigt. Sie können das Bereinigungsintervall über die SuperAgent-Richtlinie konfigurieren.

Umgang mit Kommunikationsunterbrechungen

Wenn ein SuperAgent eine Anfrage für möglicherweise veraltete Inhalte empfängt, wird vom SuperAgent eine Verbindung mit dem McAfee ePO-Server hergestellt, um zu ermitteln, ob neue Inhalte verfügbar sind. Wenn es bei den Verbindungsversuchen zu einer Zeitüberschreitung kommt, werden vom SuperAgent stattdessen die Inhalte aus seinem eigenen Repository verteilt. Dadurch soll sichergestellt werden, dass die anfordernde Seite Inhalte erhält, selbst wenn diese möglicherweise veraltet sind.

- Verwenden Sie das SuperAgent-Caching nicht mit globaler Aktualisierung. Beide erfüllen in einer verwalteten Umgebung die gleiche Funktion – sie halten die verteilten Repositories auf dem aktuellen Stand. Sie ergänzen sich jedoch nicht gegenseitig. Setzen Sie SuperAgent-Caching ein, wenn vor allem die Bandbreitenauslastung begrenzt werden soll. Globale Aktualisierung können Sie verwenden, wenn besonders Wert auf schnelle Aktualisierungen im Unternehmen gelegt wird. Ausführlichere Informationen zur globalen Aktualisierung finden Sie in der ePO-Produktdokumentation.
- SuperAgent-Caching sollte nicht zusammen mit Repository-Replizierungen verwendet werden.

Hierarchie von SuperAgents

Eine Hierarchie von SuperAgents kann Agenten, die sich im gleichen Netzwerk befinden, bei einer Minimierung der Netzwerkauslastung helfen.

Mit einem SuperAgent werden die Inhaltsaktualisierungen vom McAfee ePO-Server oder aus dem verteilten Repository im Cache gespeichert und an Agenten im Netzwerk weitergegeben, wodurch die Last auf dem McAfee ePO-Server reduziert wird. Im Idealfall sollten mehrere SuperAgents vorhanden sein, um die Netzwerklast optimal zu verteilen.

Vor dem Einrichten der **SuperAgent**-Hierarchie müssen Sie sich vergewissern, dass das verzögerte Caching aktiviert ist.

Erstellen einer Hierarchie von SuperAgents

Sie können die Hierarchie mithilfe der Repository-Richtlinie erstellen. McAfee Es wird empfohlen, eine dreistufige Hierarchie von SuperAgents im Netzwerk zu erstellen.

Durch eine Hierarchie von SuperAgents verhindern Sie, dass identische Inhaltsaktualisierungen mehrmals vom McAfee ePO-Server oder aus dem verteilten Repository heruntergeladen werden. In einem Client-Netzwerk mit mehreren SuperAgents (SuperAgent 1, SuperAgent 2, SuperAgent 3 und SuperAgent 4) sowie einem verteilten Repository können Sie die Hierarchie beispielsweise so konfigurieren, dass die Client-Systeme die Inhaltsaktualisierungen von den jeweiligen SuperAgents (SuperAgent 2, SuperAgent 3 oder SuperAgent 4) erhalten. Auf den SuperAgents 2, 3 und 4 werden Aktualisierungen von SuperAgent 1 empfangen und im Cache abgelegt. Auf SuperAgent 1 werden Aktualisierungen aus dem verteilten Repository empfangen und im Cache abgelegt.

- Im obigen Beispiel sind SuperAgent 2, SuperAgent 3 und SuperAgent 4 als SuperAgents für Client-Systeme in ihrer jeweiligen Übertragungsdomäne konfiguriert.
- Inhalte aus HTTP- oder -FTP-Repositories von McAfee können von den SuperAgents nicht im Cache abgelegt werden.

Beim Erstellen einer Hierarchie müssen Sie darauf achten, dass die Hierarchie keinen Kreis aus SuperAgents bildet. Ein solcher Kreis würde zum Beispiel gebildet, wenn SuperAgent 1 so konfiguriert ist, dass Aktualisierungen von SuperAgent 2 abgerufen werden, SuperAgent 2 so konfiguriert ist, dass Aktualisierungen von SuperAgent 3 abgerufen werden, und SuperAgent 3 wiederum so konfiguriert ist, dass Aktualisierungen von SuperAgent 1 abgerufen werden.

Damit sichergestellt ist, dass der übergeordnete SuperAgent immer über die neuesten Inhaltsaktualisierungen verfügt, muss die Übertragung von SuperAgent-Reaktivierungen aktiviert sein.

Wenn die Agenten von den SuperAgents nicht mit den neuesten Inhaltsaktualisierungen versorgt werden, weichen die Agenten auf das nächste in der Richtlinie konfigurierte Repository aus.

Anordnen von SuperAgents in einer Hierarchie

Allgemeine Richtlinien und Repository-Richtlinien können so geändert werden, dass eine SuperAgent-Hierarchie aktiviert und festgelegt werden kann.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Richtlinie** | **Richtlinienkatalog**, und wählen Sie dann im Dropdown-Menü **Produkt** den Eintrag **McAfee Agent** sowie im Dropdown-Menü **Kategorie** den Eintrag **Allgemein** aus.

2 Klicken Sie auf die Richtlinie **My Default**, um die Richtlinie zu bearbeiten. Zum Erstellen einer Richtlinie klicken Sie auf **Aktionen** | **Neue Richtlinie**.

Die Richtlinie **McAfee Default** kann nicht geändert werden.

3 Wählen Sie auf der Registerkarte **SuperAgent** die Option **Agenten in SuperAgents konvertieren** aus, um den Agenten in einen **SuperAgent** umzuwandeln und das zugehörige Repository mit den neuesten Inhalten zu aktualisieren.

4 Wählen Sie **Systeme mit SuperAgents als verteilte Repositories verwenden** aus, um die Systeme, auf denen sich SuperAgents befinden, als Aktualisierungs-Repositories für die Systeme in deren Übertragungssegment zu verwenden. Geben Sie dann den **Repository-Pfad** an.

5 Wählen Sie **Verzögertes Caching aktivieren** aus, damit SuperAgents die vom McAfee ePO-Server empfangenen Inhalte im Cache ablegen können.

6 Klicken Sie auf **Speichern**.

Auf der Seite **Richtlinienkatalog** werden die unter **Allgemein** eingestuften Richtlinien aufgeführt.

7 Ändern Sie die **Kategorie** in **Repository**, und klicken Sie dann auf die Richtlinie **My Default**, um mit dem Bearbeiten der Richtlinie zu beginnen. Wenn Sie eine Richtlinie erstellen möchten, klicken Sie auf **Aktionen** | **Neue Richtlinie**.

8 Aktivieren Sie auf der Registerkarte Repositories die Option **Reihenfolge in der Repository-Liste verwenden**.

9 Klicken Sie auf **Zugriff von Clients auf neu hinzugefügte Repositories automatisch zulassen**, um neue SuperAgent-Repositories der Liste hinzuzufügen. Klicken Sie dann auf **Zum Anfang**, um die SuperAgents hierarchisch anzuordnen.

Sortieren Sie die Repositories so, dass der übergeordnete SuperAgent immer ganz oben in der Repository-Liste steht.

10 Klicken Sie auf **Speichern**.

Nach dem Festlegen der SuperAgent-Hierarchie können Sie den Task McAfee Agent-Statistik erstellen und ausführen, um einen Bericht über die Einsparungen bei der Netzwerkbandbreite zu erstellen.

McAfee Agent-Relay-Funktionalität

Wenn die Kommunikation zwischen McAfee Agent und dem McAfee ePO-Server durch eine Netzwerkkonfiguration blockiert wird, können mit McAfee Agent keine Aktualisierungen von Inhalten und Richtlinien empfangen oder Ereignisse gesendet werden.

Zur Überbrückung der Kommunikation zwischen den Client-Systemen und dem McAfee ePO-Server kann bei McAfee Agent mit direkter Verbindung zum McAfee ePO-Server oder zum Agenten-Handler die Relay-Funktionalität aktiviert werden. Sie können auch mehr als einen McAfee Agent als Agenten vom Typ RelayServer konfigurieren, um die Netzwerklast gleichmäßiger zu verteilen.

Kommunizieren über einen RelayServer

Wenn Sie die Relay-Funktion im Netzwerk aktivieren, wird McAfee Agent in einen RelayServer umgewandelt. Mit McAfee Agent mit Relay-Funktion können Sie auf den McAfee ePO-Server oder den **RelayServer** zugreifen, die in `SiteList.xml` aufgelistet sind.

Wenn keine Verbindung zwischen McAfee Agent und dem McAfee ePO-Server hergestellt werden kann, wird eine Nachricht gesendet, um eine McAfee Agent-Instanz mit Relay-Funktion im jeweiligen Netzwerk zu erkennen. Von jedem RelayServer wird eine Antwort auf die Nachricht gesendet, und von McAfee Agent wird eine Verbindung mit dem ersten antwortenden RelayServer hergestellt.

Wenn später keine Verbindung zwischen McAfee Agent und dem McAfee ePO-Server hergestellt werden kann, wird versucht, eine Verbindung zu dem RelayServer herzustellen, der zuerst auf die Erkennungsnachricht geantwortet hat. In McAfee Agent werden diese einzelnen RelayServer im Netzwerk bei jeder Agent-Server-Kommunikation erkannt, und die Details der ersten fünf eindeutigen Server, die auf die Erkennungsnachricht geantwortet haben, werden zwischengespeichert. Wenn keine Verbindung zwischen dem aktuellen RelayServer und dem McAfee ePO-Server hergestellt werden kann oder die erforderliche Inhaltsaktualisierung fehlt, wird über McAfee Agent eine Verbindung mit dem nächsten verfügbaren RelayServer im Cache hergestellt. Aktivieren Sie die Richtlinienoption **Relay-Kommunikation aktivieren**, um die Erkennung der RelayServer durch das Client-System zuzulassen.

Wenn für die Kommunikation von McAfee Agent mit dem McAfee ePO-Server Relay verwendet wird, werden die Verbindungen in zwei Teilen hergestellt; erstens zwischen McAfee Agent und dem RelayServer, zweitens zwischen dem RelayServer und dem McAfee ePO-Server. Diese Verbindungen werden für die Dauer der Kommunikation aufrechterhalten.

Aktivieren der Relay-Funktionalität

Zum Aktivieren der Relay-Funktionalität in einem Agenten können Sie Richtlinien konfigurieren und zuweisen.

Wenn Sie ein System mit einem Nicht-Windows-Betriebssystem als RelayServer aktivieren, müssen Sie darauf achten, manuell eine Ausnahme für den Prozess `macmnsvc` und den Service-Manager-Port zu `iptables` und `ip6tables` hinzuzufügen.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Systeme**, und wählen Sie dann unter Systemstruktur eine Gruppe aus. Alle Systeme aus dieser Gruppe werden im Detailbereich angezeigt.
2. Wählen Sie ein System aus, und klicken Sie auf **Aktionen** | **Agent** | **Richtlinien auf einem einzelnen System ändern**. Die Seite Richtlinienzuweisung für dieses System wird angezeigt.
3. Wählen Sie in der Dropdown-Liste mit den Produkten den Eintrag **McAfee Agent** aus. Die Richtlinienkategorien unter McAfee Agent werden mit der dem System zugewiesenen Richtlinie aufgeführt.

4 Wenn die Richtlinie geerbt wurde, aktivieren Sie die Option **Vererbung unterbrechen und ab hier Richtlinie und Einstellungen zuweisen**.

5 Wählen Sie in der Dropdown-Liste **Zugewiesene Richtlinie** eine Richtlinie vom Typ **Allgemein** aus.

Von diesem Speicherort können Sie die ausgewählte Richtlinie bearbeiten oder eine Richtlinie erstellen.

6 Legen Sie fest, ob die Richtlinienvererbung gesperrt werden soll, um zu verhindern, dass Systemen, die diese Richtlinie erben, eine andere Richtlinie zugewiesen wird.

7 Wählen Sie auf der Registerkarte SuperAgent nach Bedarf die folgenden Optionen aus

- Wählen Sie **Relay-Kommunikation aktivieren** aus, um die Erkennung von RelayServern im Netzwerk durch Agenten zuzulassen.
- Wählen Sie **RelayServer aktivieren** aus, um die Relay-Funktionalität auf einem Agenten zu aktivieren.

- Vergewissern Sie sich, dass der **Service-Manager-Port** auf **8082** eingestellt ist.
- McAfee empfiehlt, die Relay-Funktionalität im Netzwerk Ihres Unternehmens zu aktivieren.
- Mit einem RelayServer kann keine Verbindung mit den McAfee ePO-Servern über Proxy-Einstellungen hergestellt werden.

8 Klicken Sie auf **Speichern**.

9 Senden Sie einen McAfee Agent-Reaktivierungsaufruf.

- Nach dem ersten ASKI wird der Status des RelayServers auf der Seite McAfee Agent-Eigenschaften oder in der McTray-Benutzeroberfläche auf dem Client-System aktualisiert.
- Die Protokolldatei `Macmnsvc_<hostname>.log` wird in den folgenden Speicherorten gespeichert.
  - Auf einem Windows-Client-System: `<ProgramData>\McAfee\Agent\Logs`
  - Auf einem Nicht-Windows-Client-System: `/var/McAfee/agent/logs`

Deaktivieren der Relay-Funktionalität

Sie können die Richtlinie **Allgemein** verwenden, um die Relay-Funktionalität in McAfee Agent zu deaktivieren.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Systeme**, und wählen Sie dann unter der **Systemstruktur** eine Gruppe aus. Alle Systeme aus dieser Gruppe werden im Detailbereich angezeigt.

2 Wählen Sie das System aus, auf dem die Relay-Funktionalität aktiviert war, und klicken Sie dann auf **Aktionen** | **Agent** | **Richtlinien auf einem einzelnen System ändern**. Die Seite **Richtlinienzuweisung** für dieses System wird angezeigt.

3 Wählen Sie in der Dropdown-Liste mit den Produkten den Eintrag **McAfee Agent** aus. Die Richtlinienkategorien unter **McAfee Agent** werden mit der dem System zugewiesenen Richtlinie aufgeführt.

4 Wählen Sie in der Dropdown-Liste **Zugewiesene Richtlinie** die Richtlinie **Allgemein** aus, die auf dem Client-System erzwungen wird, und deaktivieren Sie die Richtlinie.

5 Deaktivieren Sie auf der Registerkarte **SuperAgent** nach Bedarf die folgenden Optionen

- Deaktivieren Sie die Option **Relay-Kommunikation aktivieren**, um die Erkennung der **RelayServer** im Netzwerk durch Agenten anzuhalten.
- Deaktivieren Sie **RelayServer aktivieren**, um die Relay-Funktion in McAfee Agent zu deaktivieren.

6 Klicken Sie auf **Speichern**.

7 Senden Sie einen McAfee Agent-Reaktivierungsaufruf.

Peer-to-Peer-Kommunikation

Zum Abrufen von Aktualisierungen und zum Installieren von Produkten ist eine Kommunikation zwischen McAfee Agent und dem McAfee ePO-Server erforderlich. Diese Aktualisierungen sind möglicherweise mit den Agenten in derselben Übertragungsdomäne verfügbar. Durch das Herunterladen dieser Aktualisierungen von den gleichrangigen Agenten in derselben Übertragungsdomäne wird die Last auf McAfee ePO reduziert.

Herunterladen von Inhaltsaktualisierungen von gleichrangigen Agenten

Sie können die Peer-to-Peer-Kommunikation in McAfee Agent über die Richtlinie Allgemein aktivieren.

McAfee Agent kann nach Bedarf mithilfe der Richtlinie als Peer-to-Peer-Server und/oder -Client konfiguriert werden. Durch die Konfiguration von McAfee Agent als Peer-to-Peer-Server können auf Anforderung Aktualisierungen an andere in der Übertragungsdomäne bereitgestellt werden. Ein Peer-to-Peer-Server verfügt über lokalen Speicherplatz, der für das Caching der Aktualisierungen zugewiesen ist. Der Standardspeicherplatz umfasst 512 MB. Dies können Sie jedoch mithilfe der Richtlinie konfigurieren. Auf dem Peer-to-Peer-Server werden standardmäßig Aktualisierungen in `<Ordner für Agentendaten>\Daten\mcafeeP2P` zwischengespeichert. Dieser Pfad kann jedoch mithilfe der Richtlinie angepasst werden. Sie können die Richtlinie auch so konfigurieren, dass die auf dem lokalen Datenträger zwischengespeicherten Aktualisierungen bereinigt werden.

Wenn eine Inhaltsaktualisierung für einen Agenten erforderlich ist, wird versucht, Peer-to-Peer-Server mit der Inhaltsaktualisierung in der Übertragungsdomäne zu erkennen. Bei Empfang der Anfrage wird auf den als Peer-to-Peer-Server konfigurierten Agenten überprüft, ob die angefragten Inhalte auf ihnen vorhanden sind, und eine Antwort an den Agenten gesendet. Auf dem Agenten, von dem die Inhaltsanfrage ausging, wird der Inhalt von dem Peer-to-Peer-Server heruntergeladen, der zuerst geantwortet hat.

Aktivieren Sie die Richtlinienoption **Peer-to-Peer-Kommunikation aktivieren**, um die Erkennung der Peer-to-Peer-Server in der Übertragungsdomäne durch das Client-System zuzulassen.

Auf dem Peer-to-Peer-Server werden Inhalte über HTTP für Clients bereitgestellt.

Wenn die Inhaltsaktualisierung unter den Peers in der Übertragungsdomäne nicht mit McAfee Agent gefunden werden kann, wird auf das Repository zurückgewichen, wie in der Richtlinie konfiguriert.

Für die Peer-to-Peer-Kommunikation wird Port 8082 für die Erkennung von gleichrangigen Servern und Port 8081 für die Bereitstellung von Aktualisierungen an gleichrangige Agenten verwendet.

Bewährte Vorgehensweisen für die Peer-to-Peer-Kommunikation

Berücksichtigen Sie die folgenden Empfehlungen, wenn Sie die Peer-to-Peer-Kommunikation in Ihrem Netzwerk aktivieren.

- Sie sollten Peer-to-Peer-Server auf PCs oder virtuellen Systemen aktivieren. Die Aktivierung des Peer-to-Peer-Servers auf Laptops oder anderen mobilen Geräten ist nicht empfehlenswert.
- Sie sollten Peer-to-Peer-Server auf den Systemen deaktivieren, die über eine schlechte Netzwerkverbindung verfügen oder über VPN verbunden sind.
- Bei der Bereitstellung von McAfee Agent oder verwalteten Produkten oder bei der Aktualisierung der Produkte auf einer großen Anzahl von Systemen sollten Sie Peer-to-Peer-Server auf allen Systemen aktivieren. Damit wird der Netzwerkdatenverkehr im lokalen Subnetz während der Bereitstellung oder Aktualisierung beschränkt.
- Die Peer-to-Peer-Kommunikation ist standardmäßig aktiviert. Wenn Ihr Unternehmen die Peer-to-Peer-Kommunikation einschränkt, deaktivieren Sie die Peer-to-Peer-Richtlinie.
- Sie sollten die Option **Max. Datenträgerkontingent** immer auf einen größeren Wert festlegen als die Summe der normalerweise verwendeten Anwendungen und Aktualisierungen (wenn beispielsweise die DAT-Dateigröße 150 MB und durchschnittliche Produktaktualisierungsgröße 100 MB beträgt, sollte das Peer-to-Peer-Datenträgerkontingent größer als 250 MB sein).

Aktivieren des Peer-to-Peer-Diensts

Aktivieren Sie den Peer-to-Peer-Dienst in Ihrer Übertragungsdomäne, um die Last auf dem McAfee ePO-Server zu reduzieren.

Der Peer-to-Peer-Dienst ist standardmäßig aktiviert.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Systeme**, und wählen Sie dann unter Systemstruktur eine Gruppe aus. Alle Systeme aus dieser Gruppe werden im Detailbereich angezeigt.
2. Wählen Sie ein System aus, und klicken Sie auf **Aktionen** | **Agent** | **Richtlinien auf einem einzelnen System ändern**. Die Seite Richtlinienzuweisung für dieses System wird angezeigt.
3. Wählen Sie in der Dropdown-Liste mit den Produkten den Eintrag **McAfee Agent** aus. Die Richtlinienkategorien unter McAfee Agent werden mit der dem System zugewiesenen Richtlinie aufgeführt.
4. Wenn die Richtlinie geerbt wurde, wählen Sie die Option **Vererbung unterbrechen und ab hier Richtlinie und Einstellungen zuweisen** aus.
5. Wählen Sie in der Dropdown-Liste **Zugewiesene Richtlinie** eine Richtlinie vom Typ **Allgemein** aus.

   Von diesem Speicherort können Sie die ausgewählte Richtlinie bearbeiten oder eine Richtlinie erstellen.

6. Wählen Sie aus, ob die Richtlinienvererbung gesperrt werden soll, um zu verhindern, dass Systemen, die diese Richtlinie erben, eine andere Richtlinie zugewiesen wird.
7. Wählen Sie auf der Registerkarte **Peer-to-Peer** nach Bedarf die folgenden Optionen aus
   - Wählen Sie **Peer-to-Peer-Kommunikation aktivieren** aus, um die Erkennung und Verwendung von Peer-to-Peer-Servern im Netzwerk durch McAfee Agent zuzulassen.
   - Wählen Sie **Peer-to-Peer-Dienst aktivieren** aus, um die Bereitstellung von Inhalten für gleichrangige Agenten durch McAfee Agent zu aktivieren.

8 Klicken Sie auf **Speichern**.

9 Senden Sie einen McAfee Agent-Reaktivierungsaufruf.

Erfassen von McAfee Agent-Statistiken

Führen Sie den Client-Task McAfee Agent-Statistiken auf den verwalteten Knoten aus, um **RelayServer**-Statistiken und die durch die **Peer-to-Peer**-Kommunikation und **SuperAgent**-Hierarchie eingesparte Netzwerkbandbreite zu erfassen.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Systeme**, und wählen Sie dann unter der **Systemstruktur** eine Gruppe aus. Alle Systeme aus dieser Gruppe werden im Detailbereich angezeigt.

2 Wählen Sie ein System aus, und klicken Sie auf **Aktionen** | **Agent** | **Tasks auf einem einzelnen System ändern**. Die diesem System zugewiesenen Client-Tasks werden angezeigt.

3 Klicken Sie auf **Aktionen** | **Neue Client-Task-Zuweisung**.

4 Wählen Sie in der Produktliste die Option **McAfee Agent** aus, und wählen Sie dann **McAfee Agent-Statistik** als **Task-Typ** aus.

5 Klicken Sie auf **Neuen Task erstellen**. Die Seite Neuer Client-Task wird angezeigt.

6 Wählen Sie die erforderliche Option aus, und klicken Sie dann auf **Speichern**.

Wenn der Task auf dem Client-System bereitgestellt und der Status an ePolicy Orchestrator berichtet wurde, wird die Statistik auf 0 zurückgesetzt.

Zum Anzeigen der von McAfee Agent erfassten Statistiken erstellen Sie eine neue **Informationen zur Agenten-Statistik**-Abfrage, und führen Sie diese aus.

Ändern der in der Benutzeroberfläche und dem Ereignisprotokoll des Agenten verwendeten Sprache

Wenn verwaltete Systeme in einer anderen Sprache ausgeführt werden, als von Ihren Administratoren verstanden wird, kann sich die Fehlerbehebung auf diesen Systemen schwierig gestalten.

Die auf einem System in der Benutzeroberfläche und dem Ereignisprotokoll des Agenten verwendete Sprache können Sie über eine ePolicy Orchestrator-Richtlinie ändern. Diese Einstellung zwingt den Agenten auf dem Zielsystem dazu, Protokolleinträge in der ausgewählten Sprache auszuführen und zu veröffentlichen.

Einige Texte werden von einzelnen McAfee-Sicherheits-Software-Produkten (z. B. VirusScan) gesteuert und folgen den lokalen Einstellungen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Richtlinie** | **Richtlinienkatalog**.

2 Wählen Sie in der Dropdown-Liste **Produkt** den Eintrag **McAfee Agent** und in der Dropdown-Liste **Kategorie** den Eintrag **Fehlerbehebung** aus.

3 Klicken Sie auf den Namen einer Richtlinie, um sie zu ändern, oder duplizieren Sie eine vorhandene Richtlinie.

   Die Richtlinie **McAfee Default** kann nicht geändert werden.

4 Aktivieren Sie **Wählen Sie die vom Agenten verwendete Sprache aus**, und wählen Sie eine Sprache in der Dropdown-Liste aus.

5 Klicken Sie auf **Speichern**.

Wenn Sie diese Richtlinie einem System zuweisen, wird der Agent auf diesem System in der ausgewählten Sprache ausgeführt und nimmt Protokolleinträge in dieser Sprache vor. Falls diese Sprache nicht mit dem aktuellen Windows-Systemgebietsschema übereinstimmt, sind die im **Agenten-Monitor** angezeigten Protokollmeldungen möglicherweise nicht lesbar.

Unabhängig von der Sprachauswahl werden einige Protokollmeldungen immer in Englisch veröffentlicht, um McAfee bei der Behebung von Kundenproblemen zu helfen.

Konfigurieren von ausgewählten Systemen für die Aktualisierung

Sie können einen Satz von Paketen auswählen, die sofort aktualisiert werden, wenn **Jetzt aktualisieren** auf einem oder mehreren Systemen vom ePolicy Orchestrator-Server ausgewählt wird.

Zu den häufigen Gründen für die Verwendung dieser Funktionalität gehören u. a.:

- Aktualisieren von ausgewählten Systemen bei der Fehlerbehebung
- Sofortiges Verteilen neuer DAT-Dateien oder Signaturen auf eine große Anzahl von Systemen oder alle Systeme
- Aktualisieren ausgewählter Produkte, Patches oder Service Packs, die zu einem früheren Zeitpunkt ausgebracht wurden

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur**, und wählen Sie dann die Systeme aus, die aktualisiert werden sollen.

2 Klicken Sie auf **Aktionen** | **Agent** | **Jetzt aktualisieren**.

- Wählen Sie **Alle Pakete** aus, um alle Aktualisierungspakete in das Repository auszubringen.
- Wählen Sie **Ausgewählte Pakete** aus, um anzugeben, welche Aktualisierungspakete ausgebracht werden sollen. Heben Sie die Auswahl der Pakete auf, die nicht ausgebracht werden sollen.

Mithilfe der Fähigkeit, Patches und Service Packs aus den Repositories **Test** oder **Vorherige** auszubringen, soll es ermöglicht werden, Aktualisierungen auf einer begrenzten Anzahl von Systemen zu testen, bevor eine breitere Ausbringung erfolgt. McAfee empfiehlt, genehmigte Patches und Service Packs in das Repository **Aktuell** zu verschieben, wenn sie zur allgemeinen Ausbringung bereit sind.

3 Klicken Sie auf **OK**.

Antworten auf Richtlinienereignisse

Sie können eine automatische Reaktion in McAfee ePO einrichten, die so gefiltert wird, dass nur Richtlinienereignisse angezeigt werden.

Ausführlichere Informationen über **Automatische Reaktionen** finden Sie in der ePO-Produktdokumentation.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Automatisierung** | **Automatische Reaktionen**, um die Seite Automatische Reaktionen zu öffnen.

2 Klicken Sie auf **Aktionen** | **Neue Antwort**.

3 Geben Sie einen **Namen** für die Antwort und eine optionale **Beschreibung** ein.

4 Wählen Sie bei der **Ereignisgruppe** den Eintrag **ePO-Benachrichtigungsereignisse** und beim **Ereignistyp** den Eintrag **Client, Bedrohung** oder **Server** aus.

5 Klicken Sie auf **Aktiviert**, um die Reaktion zu aktivieren, und klicken Sie dann auf **Weiter**.

6 Wählen Sie in **Verfügbare Eigenschaften** die Option **Ereignisbeschreibung** aus.

7 Klicken Sie in der Zeile **Ereignisbeschreibung** auf die Schaltfläche zum Durchsuchen (…), und wählen Sie eine der folgenden Optionen aus:

- **Fehler des Agenten beim Erfassen der Eigenschaften von Einzelprodukten**: Dieses Ereignis wird generiert und weitergeleitet, wenn erstmals ein Fehler bei der Eigenschaftserfassung auftritt. Ein nachfolgendes Ereignis vom Typ Erfolg wird nicht generiert. Für jeden Fehler bei einem verwalteten Produkt wird ein eigenes Ereignis generiert.
- **Fehler des Agenten beim Erzwingen der Richtlinie für Einzelprodukte**: Dieses Ereignis wird generiert und weitergeleitet, wenn erstmals ein Fehler bei der Richtlinienerzwingung auftritt. Ein nachfolgendes Ereignis vom Typ Erfolg wird nicht generiert. Für jeden Fehler bei einem verwalteten Produkt wird ein eigenes Ereignis generiert.

8 Geben Sie gegebenenfalls die restlichen Informationen in den Filter ein, und klicken Sie dann auf **Weiter**.

9 Wählen Sie die Optionen **Aggregation**, **Gruppierung** und **Beschränkung** je nach Bedarf aus.

10 Wählen Sie einen Aktionstyp aus, geben Sie das gewünschte Verhalten je nach Aktionstyp ein, und klicken Sie dann auf **Weiter**.

11 Überprüfen Sie die Zusammenfassung des Antwortverhaltens. Wenn alles korrekt ist, klicken Sie auf **Speichern**.

Bei der automatischen Reaktion wird die beschriebene Aktion ausgeführt, wenn ein Richtlinienereignis auftritt.

Planen von Client-Tasks

Beim Zuweisen eines Client-Tasks zu einem System oder einer Gruppe von Systemen in der Systemstruktur können Sie die Ausführung der Tasks auf der Basis verschiedener Parameter planen.

Auf der Registerkarte Plan im Generator für Client-Task-Zuweisung können Sie konfigurieren, ob der Task gemäß seinem Plan ausgeführt werden soll. Wenn das Planen deaktiviert ist, kann der Task nur ausgehend von der Seite **Systemstruktur** | **Systeme** ausgeführt werden, entweder durch Klicken auf **Aktionen** | **Agent** | **Agent** | **Client-Task jetzt ausführen** oder als Server-Task-Aktion.

Die Ausführung von Client-Tasks kann zu den folgenden Zeitintervallen geplant werden:

- **Täglich**: Gibt an, dass der Task entweder jeden Tag zu einer bestimmten Uhrzeit, regelmäßig zwischen zwei Uhrzeiten des Tages oder als Kombination beider Möglichkeiten ausgeführt wird.
- **Wöchentlich**: Gibt an, dass der Task jede Woche ausgeführt wird. Ein wöchentlicher Task kann so geplant werden, dass er an einem bestimmten Wochentag, an allen Wochentagen, an Wochenenden oder als Kombination dieser Möglichkeiten ausgeführt wird. Sie können einen wöchentlichen Task für die Ausführung zu einer bestimmten Uhrzeit an den ausgewählten Tagen oder für eine regelmäßige Ausführung zwischen zwei Uhrzeiten der ausgewählten Tage planen.
- **Monatlich**: Gibt an, dass der Task jeden Monat ausgeführt wird. Ein monatlicher Task kann so geplant werden, dass er zu einer bestimmten Uhrzeit an einem oder mehreren spezifischen Tagen des jeweiligen Monats ausgeführt wird.
- **Einmal**: Startet den Task zum angegebenen Datum und Zeitpunkt.
- **Bei Systemstart**: Startet den Task beim nächsten Start des Servers.
- **Bei Anmeldung**: Starten den Task, wenn Sie sich das nächste Mal beim Server anmelden.
- **Sofort ausführen**: Startet den Task sofort.

Nachdem der Task zum ersten Mal ausgeführt wurde, wird er nicht noch einmal ausgeführt.

Zusätzlich können Sie die folgenden Aktionen durchführen:

- Konfigurieren Sie das Start- und Enddatum, zu dem der Client-Task zur Ausführung zu den geplanten Intervallen verfügbar oder nicht verfügbar ist.
- Geben Sie die Zeit an, zu der der Task beginnen sollte.
- Geben Sie an, ob der Task nur einmal zur Startzeit ausgeführt oder bis zu einem späteren Zeitpunkt weitergeführt werden soll. Sie können auch das Intervall angeben, in dem der Task innerhalb dieser Zeit ausgeführt wird.
- Geben Sie an, ob der Task nach der lokalen Zeit des verwalteten Systems oder nach der koordinierten Weltzeit (Coordinated Universal Time (UTC)) ausgeführt werden soll.
- Konfigurieren Sie das Task-Verhalten und die Aktion, die durchgeführt werden soll, wenn der Task zu lange ausgeführt wird, oder geben Sie an, ob der Task ausgeführt werden soll, falls er ausgelassen wurde.

Ausführliche Informationen zum Zuweisen und Planen eines Client-Tasks finden Sie in der ePolicy Orchestrator-Produktdokumentation.

Sofortiges Ausführen von Client-Tasks

Wenn eine Kommunikation zwischen dem McAfee ePO-Server und McAfee Agent stattfindet, können Sie über die Aktion **Client-Task jetzt ausführen** Client-Tasks sofort ausführen.

Tasks werden von McAfee Agent nicht sofort nach der Planung ausgeführt, sondern in eine Warteschlange eingereiht. Während dieses Platzieren in einer Warteschlange sofort erfolgt, wird mit der Ausführung eines Tasks nur dann auch begonnen, wenn sich in der Warteschlange keine weiteren Tasks vor ihm befinden. Im Rahmen des Verfahrens **Client-Task jetzt ausführen** erstellte Tasks werden ausgeführt, und der Task wird nach Abschluss auf dem Client gelöscht.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur**.

2 Wählen Sie ein oder mehrere Systeme aus, auf denen ein Task ausgeführt werden soll.

3 Klicken Sie auf **Aktionen** | **Agent** | **Client-Task jetzt ausführen**.

4 Wählen Sie bei **Produkt** den Eintrag **McAfee Agent** sowie den **Task-Typ** aus.

5 Zum Ausführen eines vorhandenen Tasks klicken Sie auf den entsprechenden **Task-Namen** und dann auf **Task jetzt ausführen**.

6 Zum Definieren eines neues Tasks klicken Sie auf **Neuen Task erstellen**.

   a Geben Sie die entsprechenden Informationen zu dem Task ein, den Sie erstellen.

> Wenn Sie bei dieser Vorgehensweise einen McAfee Agent **Produktbereitstellungs**- oder **Produktaktualisierungs**-Task erstellen, ist die Option **Bei jeder Richtlinienerzwingung ausführen** verfügbar. Diese Option hat keine Auswirkungen, da der Task nach seinem Abschluss gelöscht wird.

Die Seite **Client-Task-Ausführungsstatus** wird angezeigt, die den Status aller ausgeführten Tasks enthält. Wenn die Tasks abgeschlossen sind, können Sie die Ergebnisse im **Audit-Protokoll** und im **Server-Task-Protokoll** anzeigen.

Ermitteln inaktiver Agenten

Eine inaktive McAfee Agent-Instanz ist ein Agent, der innerhalb eines vom Benutzer angegebenen Zeitraums nicht mit dem McAfee ePO-Server kommuniziert hat.

Einige Agenten können von Endbenutzern deaktiviert oder deinstalliert werden. Es kann auch vorkommen, dass das System, auf dem McAfee Agent gehostet wird, aus dem Netzwerk entfernt wird. McAfee empfiehlt, regelmäßig (wöchentlich) nach Systemen mit inaktiven Agenten zu suchen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Berichterstellung** | **Abfragen und Berichte**.

2 Wählen Sie in der Liste **Gruppen** die freigegebene Gruppe **Agentenverwaltung** aus.

3 Klicken Sie in der Zeile **Inaktive Agenten** auf **Ausführen**, um die Abfrage auszuführen.

   In der Standardkonfiguration werden mit dieser Abfrage Systeme gesucht, die im letzten Monat nicht mit dem McAfee ePO-Server kommuniziert haben. Sie können diese Standardabfrage duplizierten und ändern, um Stunden, Tage, Wochen, Quartale oder Jahre anzugeben.

Wenn Sie inaktive Agenten finden, überprüfen Sie deren Aktivitätsprotokolle auf Probleme, die die Ursache für die gestörte Agent-Server-Kommunikation sein könnten. Mithilfe der Abfrageergebnisse können Sie verschiedene Aktionen für die ermittelten Systeme durchführen (z. B. Senden eines Ping-Befehls, Löschen, Reaktivieren und erneutes Bereitstellen von McAfee Agent).

Windows-Systeme und vom Agenten gemeldete Produkteigenschaften

Von McAfee Agent werden Systemeigenschaften aus den zugehörigen verwalteten Systemen an ePolicy Orchestrator gemeldet. Welche Eigenschaften gemeldet werden, variiert je nach Betriebssystem. Bei den aufgeführten Eigenschaften handelt es sich um von Windows gemeldete Eigenschaften.

Systemeigenschaften

Diese Liste enthält die Systemdaten, die vom Betriebssystem der Knoten an ePolicy Orchestrator gemeldet werden. Überprüfen Sie die Details auf Ihrem System, bevor Sie von einer fehlerhaften Meldung ausgehen.

Agenten-GUID
CPU-Seriennummer
CPU-Geschwindigkeit (in MHz)
CPU-Typ
Benutzerdefinierte Eigenschaften 1–4
Kommunikationstyp
Standardsprache
Beschreibung
DNS-Name
Domänenname
Ausgeschlossene Tags
Freier Speicherplatz
Freier Arbeitsspeicher
Freier Speicherplatz auf dem Systemlaufwerk
Installierte Produkte
IP-Adresse
IPX-Adresse
Ist 64-Bit-Betriebssystem
Ist Laptop
Letzter Reihenfolgefehler
Letzte Kommunikation
LDAP-Speicherort
MAC-Adresse
Status "Verwaltet"
Verwaltungstyp
Anzahl der CPUs
Betriebssystem
OS-Build-Nummer
OS-OEM-Kennung
OS-Plattform
OS-Service Pack-Version
OS-Typ
OS-Version
Server-Schlüssel
Reihenfolgefehler
Subnetzadresse
Subnetzmaske
Systembeschreibung
Systemstandort
Systemname
Systemstruktursortierung
Tags
Zeitzone
Zu übertragen
Gesamter Speicherplatz
Gesamter physischer Speicher
Belegter Speicherplatz
Benutzername
Vdi

Agenten-Eigenschaften

Für jedes McAfee-Produkt werden bestimmte Eigenschaften an ePolicy Orchestrator gemeldet. Darüber hinaus ist festgelegt, welche dieser Eigenschaften in eine Gruppe minimaler Eigenschaften aufgenommen werden. Diese Liste enthält die Arten von Produktdaten, die von der auf dem System installierten ePolicy Orchestrator-Software an McAfee gemeldet werden. Falls Sie Fehler in den gemeldeten Werten finden, überprüfen Sie zunächst die Einzelheiten Ihrer Produkte, bevor Sie von einer fehlerhaften Meldung ausgehen.

Agenten-GUID
Schlüssel-Hash für sichere Agent-Server-Kommunikation
Agent-Server-Kommunikationsintervall
Agenten-Reaktivierung
Kommunikationsport für Agenten-Reaktivierung
Cluster-Knoten
Zustand des Cluster-Dienstes
Cluster-Name
Cluster-Host
Cluster-Mitglieds-Knoten
Pfad der Cluster-Quorum-Ressource
Cluster-IP-Adresse
DAT-Version
Scan-Modul-Version
Automatischen Neustart erzwingen nach
HotFix/Patch-Version
Installationspfad
IsLazyCachingEnabled
Sprache
Status der letzten Richtlinienerzwingung
Status der letzten Eigenschaftserfassung
Lizenzstatus
Peer-to-Peer
Peer-to-Peer-Repository-Verzeichnis
Aufforderung zum Neustart, wenn erforderlich
Richtlinienerzwingungsintervall
Produktversion
Plug-In-Version
Jetzt ausführen wird unterstützt
Service Pack
McAfee-Symbol in der Taskleiste anzeigen
RelayServer
SuperAgent-Funktion
SuperAgent-Repository
Verzögerter Cache bei SuperAgents
SuperAgent-Repository-Verzeichnis
Kommunikationsport für SuperAgent-Reaktivierung

Anzeigen von McAfee Agent-Eigenschaften und Produkteigenschaften

Eine häufige Aufgabe bei der Fehlerbehebung besteht darin, zu überprüfen, dass die von Ihnen vorgenommenen Richtlinienänderungen mit den aus einem System abgerufenen Eigenschaften übereinstimmen.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur**.

2 Klicken Sie auf der Registerkarte **Systeme** auf die entsprechende Zeile des Systems, das Sie überprüfen möchten.

Es werden Informationen zu den Eigenschaften des Systems, den installierten Produkten und zum Agenten angezeigt. Oben auf der Seite Systeminformationen sehen Sie die Fenster Zusammenfassung, Eigenschaften und Bedrohungsereignisse. Außerdem werden hier die Registerkarten Systemeigenschaften, Produkte, Bedrohungsereignisse und McAfee Agent angezeigt.

Von McAfee Agent bereitgestellte Abfragen

Der McAfee ePO-Server bietet eine Reihe von Standardabfragen in Bezug auf McAfee Agent.

Die folgenden Abfragen werden in der freigegebenen Gruppe Agentenverwaltung installiert.

Tabelle 11-1 Von McAfee Agent bereitgestellte Abfragen

Abfrage	Beschreibung
Zusammenfassung Agentenkommunikation	Zeigt ein Kreisdiagramm mit verwalteten Systemen an, in dem angegeben ist, ob innerhalb des letzten Tages eine Kommunikation zwischen McAfee Agent und dem McAfee ePO-Server stattgefunden hat.
Agenten-Handler-Status	Ein Kreisdiagramm, in dem der Kommunikationsstatus des Agenten-Handlers aus der letzten Stunde angezeigt wird.
Informationen zur Agentenstatistik	Ein Balkendiagramm, in dem die folgenden McAfee Agent-Statistiken angezeigt werden: • Anzahl der fehlgeschlagenen Verbindungen zu RelayServer • Anzahl der nach der maximal erlaubten Anzahl an Verbindungen vorgenommenen Verbindungsversuche zu RelayServer • Die durch Verwendung der SuperAgent-Hierarchie eingesparte Netzwerkbandbreite
Zusammenfassung Agenten-Version	Ein Kreisdiagramm mit auf verwalteten Systemen installierten Agenten (nach Versionsnummer).
Inaktive Agenten	Eine Tabelle mit allen verwalteten Systemen, deren Agenten innerhalb des letzten Monats nicht kommuniziert haben.
Repositories und Auslastung in Prozent	Ein Kreisdiagramm, das die Auslastung einzelner Repositories in Form eines Prozentwerts aus allen Repositorys anzeigt.
Repository-Verwendung basierend auf DAT- und Scan-Modul-Abruf	Ein gestapeltes Balkendiagramm, das den Abruf von DAT- und Scan-Modul-Dateien pro Repository anzeigt.
Systeme pro Agenten-Handler	Ein Kreisdiagramm, in dem die Anzahl verwalteter Systeme pro Agenten-Handler angezeigt wird.

Verwalten der Agenten-Server-Kommunikation

Ändern Sie die Einstellungen für ePolicy Orchestrator, um die Agent-Server-Kommunikation auf die Anforderungen Ihrer Umgebung anzupassen.

Zulassen der Zwischenspeicherung von Anmeldeinformationen für die Agenten-Ausbringung

Um Agenten erfolgreich vom McAfee ePO-Server auf Systemen im Netzwerk ausbringen zu können, müssen Administratoren Anmeldeinformationen angeben. Sie können festlegen, ob die Anmeldeinformationen für die Agenten-Ausbringung für jeden Benutzer im Cache abgelegt werden sollen.

Wenn die Anmeldeinformationen eines Benutzers im Cache abgelegt werden, kann dieser Benutzer Agenten ausbringen, ohne seine Anmeldeinformationen erneut angeben zu müssen. Anmeldeinformationen werden benutzerspezifisch gespeichert, d. h. ein Benutzer kann Agenten nur dann ausbringen, wenn er seine eigenen Anmeldeinformationen zuvor schon einmal angegeben hat.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste **Einstellungskategorien** den Eintrag **Anmeldeinformationen für Agenten-Ausbringung** aus, und klicken Sie dann auf **Bearbeiten**.

2 Aktivieren Sie das Kontrollkästchen, damit die Anmeldeinformationen für die Agenten-Ausbringung im Cache abgelegt werden.

Ändern der Ports für die Agenten-Kommunikation

Einige der für die Agenten-Kommunikation verwendeten Ports auf dem McAfee ePO-Server können Sie ändern.

Die Einstellungen für die folgenden Agenten-Kommunikationsports können Sie ändern:

- **Sicherer Port für Agent-zu-Server-Kommunikation**
- **Kommunikationsport für Agenten-Reaktivierung**
- **Kommunikationsport für Agenten-Übertragung**

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste **Einstellungskategorien** den Eintrag **Ports** aus, und klicken Sie dann auf **Bearbeiten**.

2 Legen Sie fest, ob der Port 443 als sicherer Port für die Agent-zu-Server-Kommunikation aktiviert werden soll, geben Sie die Ports ein, die für Agenten-Reaktivierungen und Agenten-Übertragungen verwendet werden sollen, und klicken Sie dann auf **Speichern**.

12 Sicherheitsschlüssel

Mit Sicherheitsschlüsseln können Sie die Kommunikation und Inhalte in der von ePolicy Orchestrator verwalteten Umgebung überprüfen und authentifizieren.

Inhalt

- *Beschreibung und Funktionsweise von Sicherheitsschlüsseln*
- *Schlüsselpaar für Master-Repository*
- *Öffentliche Schlüssel für weitere Repositories*
- *Verwalten von Repository-Schlüsseln*
- *ASSC-Schlüssel (Schlüssel für sichere Agenten-Server-Kommunikation)*
- *Sichern und Wiederherstellen von Schlüsseln*

Beschreibung und Funktionsweise von Sicherheitsschlüsseln

Der McAfee ePO-Server beruht auf drei Sicherheitsschlüsselpaaren.

Die drei Sicherheitsschlüsselpaare werden für folgende Zwecke verwendet:

- Authentifizieren der Agent-zu-Server-Kommunikation
- Überprüfen der Inhalte lokaler Repositories
- Überprüfen der Inhalte remoter Repositories

Mit dem geheimen Schlüssel jedes Paares werden Nachrichten oder Pakete an ihrer Quelle signiert, während sie mit dem öffentlichen Schlüssel des Paares an ihrem Ziel überprüft werden.

ASSC-Schlüssel (Schlüssel für sichere Agenten-Server-Kommunikation)

- Wenn der Agent zum ersten Mal mit dem Server kommuniziert, sendet er seinen öffentlichen Schlüssel an den Server.
- Von diesem Zeitpunkt an verwendet der Server den öffentlichen Schlüssel des Agenten, um Nachrichten zu überprüfen, die mit dem geheimen Schlüssel des Agenten signiert wurden.
- Eigene Nachrichten signiert der Server mit seinem eigenen geheimen Schlüssel, bevor er sie an den Agenten sendet.
- Der Agent überprüft dann die Nachrichten des Servers mithilfe des öffentlichen Schlüssels des Servers.
- Es kann mehrere Schlüsselpaare für die sichere Kommunikation geben, *jedoch kann nur ein Schlüsselpaar als Master-Schlüssel festgelegt werden*.

- Wenn der Client-Task zur Agenten-Schlüsselaktualisierung (**McAfee ePO Agent Key Updater**) ausgeführt wird, erhalten Agenten, die andere öffentliche Schlüssel verwenden, den aktuellen öffentlichen Schlüssel.
- Wenn Sie ein Upgrade durchführen, werden vorhandene Schlüssel zum McAfee ePO-Server migriert.

Schlüsselpaare für lokales Master-Repository

- Mit dem geheimen Repository-Schlüssel wird das Paket signiert, bevor es in das Repository eingecheckt wird.
- Mit dem öffentlichen Repository-Schlüssel wird der Inhalt von Repository-Paketen überprüft.
- Der Agent ruft bei jedem Client-Aktualisierungs-Task verfügbare neue Inhalte ab.
- Dieses Schlüsselpaar ist für jeden Server eindeutig.
- Durch Exportieren und Importieren von Schlüsseln zwischen Servern können Sie dasselbe Schlüsselpaar in einer Umgebung mit mehreren Servern verwenden.

Andere Repository-Schlüsselpaare

- Inhalte einer vertrauenswürdigen Quelle werden mit ihrem geheimen Schlüssel signiert, bevor die Inhalte an ihr Remote-Repository gesendet werden. Zu vertrauenswürdigen Quellen gehören die McAfee-Download-Site und das SIA-Repository (Security Innovation Alliance) von McAfee.

  Wenn dieser Schlüssel gelöscht wird, können Sie keine Abrufe mehr ausführen, selbst wenn Sie einen Schlüssel von einem anderen Server importieren. Bevor Sie diesen Schlüssel überschreiben oder löschen, müssen Sie sich deshalb vergewissern, dass Sie ihn an einem geschützten Ort gesichert haben.

- Mit dem öffentlichen Schlüssel von McAfee Agent werden Inhalte überprüft, die aus dem Remote-Repository abgerufen wurden.

Schlüsselpaar für Master-Repository

Der private Schlüssel für das Master-Repository signiert alle nicht signierten Inhalte im Master-Repository. Dieser Schlüssel ist eine Funktion von Agenten ab der Version 4.0.

Agenten ab der Version 4.0 verwenden den öffentlichen Schlüssel, um Repository-Inhalte zu überprüfen, die aus dem Master-Repository auf diesem McAfee ePO-Server stammen. Wenn der Inhalt nicht signiert oder mit einem unbekannten privaten Repository-Schlüssel signiert ist, wird der heruntergeladene Inhalt als unzulässig betrachtet und gelöscht.

Dieses Schlüsselpaar ist für jede Serverinstallation eindeutig. Durch Exportieren und Importieren von Schlüsseln können Sie jedoch das gleiche Schlüsselpaar in einer Umgebung mit mehreren Servern verwenden. Mit dieser Maßnahme stellen Sie sicher, dass Agenten immer eine Verbindung mit einem der Master-Repositories herstellen können, selbst wenn ein anderes Repository heruntergefahren ist.

Öffentliche Schlüssel für weitere Repositories

Bei anderen Schlüsseln als dem Hauptschlüsselpaar handelt es sich um die öffentlichen Schlüssel, mit denen Agenten Inhalte aus anderen Master-Repositories in Ihrer Umgebung oder McAfee-Quellsites überprüfen. Jeder Agent, der sich bei diesem Server meldet, verwendet die in der Liste **Öffentliche Schlüssel für weitere Repositories** aufgeführten Schlüssel zum Überprüfen von Inhalten, die von anderen McAfee ePO-Servern in Ihrem Unternehmen oder aus McAfee-eigenen Quellen stammen.

Wenn ein Agent Inhalte herunterlädt, die aus einer Quelle stammen, für die der Agent keinen entsprechenden öffentlichen Schlüssel besitzt, verwirft der Agent den Inhalt.

Diese Schlüssel sind eine neue Funktion. Nur Agenten ab der Version 4.0 können diese neuen Protokolle verwenden.

Verwalten von Repository-Schlüsseln

Gehen Sie wie in diesen Aufgaben beschrieben vor, um Repository-Schlüssel zu verwalten.

Aufgaben

- *Verwenden eines Master-Repository-Schlüsselpaares für alle Server* auf Seite 173
  Mithilfe der Option **Server-Einstellungen** können Sie in einer Umgebung mit mehreren Servern sicherstellen, dass alle McAfee ePO-Server und Agenten dasselbe Master-Repository-Schlüsselpaar verwenden.
- *Verwenden von Schlüsseln für das Master-Repository in Umgebungen mit mehreren Servern* auf Seite 174
  Stellen Sie sicher, dass Agenten von allen McAfee ePO-Servern in der Umgebung stammende Inhalte verwenden können. Verwenden Sie dazu die Option **Server-Einstellungen**.

Verwenden eines Master-Repository-Schlüsselpaares für alle Server

Mithilfe der Option **Server-Einstellungen** können Sie in einer Umgebung mit mehreren Servern sicherstellen, dass alle McAfee ePO-Server und Agenten dasselbe Master-Repository-Schlüsselpaar verwenden.

Dazu müssen Sie das Schlüsselpaar, das von allen Servern verwendet werden soll, zuerst exportieren und dann auf allen Servern in Ihrer Umgebung importieren.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste **Einstellungskategorien** den Eintrag **Sicherheitsschlüssel** aus, und klicken Sie dann auf **Bearbeiten**.

   Die Seite **Sicherheitsschlüssel: Bearbeiten** wird angezeigt.

2 Klicken Sie neben **Schlüsselpaare für lokales Master-Repository** auf **Schlüsselpaar exportieren**.

3 Klicken Sie auf **OK**. Das Dialogfeld **Dateidownload** wird angezeigt.

4 Klicken Sie auf **Speichern**, wechseln Sie zum Speichern der ZIP-Datei mit den Schlüsseldateien für die sichere Kommunikation zu einem Speicherort, auf den von den anderen Servern aus zugegriffen werden kann, und klicken Sie dann auf **Speichern**.

5 Klicken Sie neben **Schlüssel importieren und sichern** auf **Importieren**.

6 Wechseln Sie zu der ZIP-Datei, in der sich die Dateien mit den exportierten Master-Repository-Schlüsseln befinden, und klicken Sie dann auf **Weiter**.

7 Vergewissern Sie sich, dass dies die Schlüssel sind, die Sie importieren möchten, und klicken Sie dann auf **Speichern**.

Das importierte Master-Repository-Schlüsselpaar ersetzt das vorhandene Schlüsselpaar auf diesem Server. Agenten verwenden das neue Schlüsselpaar nach dem nächsten Agenten-Aktualisierungs-Task. Nachdem das Master-Repository-Schlüsselpaar geändert wurde, muss eine sichere Agenten-Server-Kommunikation durchgeführt werden, bevor der Agent den neuen Schlüssel verwenden kann.

Verwenden von Schlüsseln für das Master-Repository in Umgebungen mit mehreren Servern

Stellen Sie sicher, dass Agenten von allen McAfee ePO-Servern in der Umgebung stammende Inhalte verwenden können. Verwenden Sie dazu die Option **Server-Einstellungen**.

Alle in das Repository eingecheckten nicht signierten Inhalte werden vom Server mit dem privaten Schlüssel für das Master-Repository signiert. Aus Repositories im Unternehmen oder von McAfee-Quellsites abgerufene Inhalte werden von Agenten mithilfe von öffentlichen Repository-Schlüsseln überprüft.

Das Schlüsselpaar für das Master-Repository ist für jede Installation von ePolicy Orchestrator eindeutig. Bei Einsatz mehrerer Server wird für jeden Server ein anderer Schlüssel verwendet. Wenn die Agenten aus unterschiedlichen Master-Repositories stammende Inhalte herunterladen können, müssen Sie sicherstellen, dass die Inhalte von den Agenten als gültig erkannt werden.

Dazu haben Sie zwei Möglichkeiten:

- Verwenden Sie für alle Server und Agenten dasselbe Schlüsselpaar für das Master-Repository.
- Stellen Sie sicher, dass Agenten so konfiguriert sind, dass alle in der Umgebung verwendeten öffentlichen Repository-Schlüssel erkannt werden.

Mit diesem Task wird das Schlüsselpaar von einem McAfee ePO-Server auf einen McAfee ePO-Zielserver exportiert und dann auf dem McAfee ePO-Zielserver importiert. Das vorhandene Schlüsselpaar wird dabei überschrieben.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf dem McAfee ePO-Server mit dem Schlüsselpaar für das Master-Repository auf **Menü** | **Konfiguration** | **Server-Einstellungen**. Wählen Sie die Option **Sicherheitsschlüssel** in der Liste **Einstellungskategorien** aus, und klicken Sie dann auf **Bearbeiten**.
2. Klicken Sie neben **Schlüsselpaar für lokales Master-Repository** auf **Schlüsselpaar exportieren** und dann auf **OK**.
3. Klicken Sie im Dialogfeld **Datei-Download** auf **Speichern**.
4. Wechseln Sie zu einem Speicherort auf dem McAfee ePO-Zielserver, an dem die ZIP-Datei gespeichert werden soll. Ändern Sie gegebenenfalls den Namen der Datei, und klicken Sie dann auf **Speichern**.
5. Klicken Sie auf dem McAfee ePO-Zielserver, auf dem Sie das Schlüsselpaar für das Master-Repository laden möchten, auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie **Sicherheitsschlüssel** in der Liste **Einstellungskategorien** aus, und klicken Sie dann auf **Bearbeiten**.

6 Führen Sie auf der Seite **Sicherheitsschlüssel bearbeiten** die folgenden Schritte aus:

   a Klicken Sie neben **Schlüssel importieren und sichern** auf **Importieren**.

   b Wechseln Sie neben **Datei auswählen** zu dem von Ihnen gespeicherten Schlüsselpaar für das Master-Repository, wählen Sie es aus, und klicken Sie dann auf **Weiter**.

   c Überprüfen Sie, ob die Zusammenfassungsinformationen richtig sind, und klicken Sie dann auf **Speichern**. Das neue Master-Schlüsselpaar wird in der Liste neben **Schlüssel für sichere Agenten-Server-Kommunikation** angezeigt.

7 Wählen Sie in der Liste die Datei aus, die Sie in den vorherigen Schritten importiert haben, und klicken Sie auf **Als Master festlegen**. Dadurch wird das neu importierte Schlüsselpaar als Hauptschlüsselpaar festgelegt.

8 Klicken Sie auf **Speichern**, um den Vorgang abzuschließen.

ASSC-Schlüssel (Schlüssel für sichere Agenten-Server-Kommunikation)

Mithilfe von ASSC-Schlüsseln (Agent-Server Secure Communication, sichere Agenten-Server-Kommunikation) können Agenten sicher mit dem Server kommunizieren.

Sie können jedes beliebige ASSC-Schlüsselpaar als Hauptschlüssel festlegen. Das ist das Schlüsselpaar, das derzeit allen ausgebrachten Agenten zugewiesen ist. Vorhandene Agenten, die andere Schlüssel in der Liste **Schlüssel für sichere Agenten-Server-Kommunikation** verwenden, wechseln nur dann zum neuen Hauptschlüssel, wenn ein Aktualisierungs-Task für Client-Agenten-Schlüssel geplant ist und ausgeführt wird.

Löschen Sie ältere Schlüssel erst dann, wenn alle Agenten den neuen Hauptschlüssel übernommen haben.

Ältere Windows-Agenten als Version 4.0 werden nicht unterstützt.

Verwalten von ASSC-Schlüsseln

Auf der Seite Server-Einstellungen können Sie Schlüssel für sichere Agenten-Server-Kommunikation (ASSC) generieren, exportieren, importieren oder löschen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Öffnen Sie die Seite Sicherheitsschlüssel: Bearbeiten.

   a Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**.

   b Wählen Sie in der Liste **Einstellungskategorien** die Option **Sicherheitsschlüssel** aus.

2 Wählen Sie eine der folgenden Aktionen aus.

Aktion	Vorgehensweise
Generieren und Verwenden neuer ASSC-Schlüsselpaare	1 Klicken Sie neben der Liste **Schlüssel für sichere Agenten-Server-Kommunikation** auf **Neuer Schlüssel**. Geben Sie in dem Dialogfeld den Namen des Sicherheitsschlüssels ein. 2 Wenn der neue Schlüssel von vorhandenen Agenten verwendet werden soll, wählen Sie den Schlüssel in der Liste aus, und klicken Sie dann auf **Als Master festlegen**. Der neue Schlüssel wird nach Abschluss des nächsten McAfee Agent-Aktualisierungs-Tasks von Agenten verwendet. Stellen Sie sicher, dass für jede McAfee Agent-Version, die von McAfee ePO verwaltet wird, ein Agenten-Schlüsselaktualisierungspaket vorhanden ist. Bei umfangreicheren Installationen sollten Sie nur dann neue Master-Schlüsselpaare generieren und verwenden, wenn es dafür gute Gründe gibt. Sie sollten dieses Verfahren phasenweise durchführen, damit Sie den Fortschritt genauer überwachen können. 3 Löschen Sie den alten Schlüssel, wenn er von keinem der Agenten mehr verwendet wird. In der Liste mit den Schlüsseln wird rechts von jedem Schlüssel angezeigt, von wie vielen Agenten er gerade verwendet wird. 4 Sichern Sie alle Schlüssel.
Exportieren von ASSC-Schlüsseln	Exportieren Sie ASSC-Schlüssel von einem McAfee ePO-Server auf einen anderen McAfee ePO-Server, um Agenten den Zugriff auf den neuen McAfee ePO-Server zu ermöglichen. 1 Wählen Sie in der Liste **Schlüssel für sichere Agenten-Server-Kommunikation** einen Schlüssel aus, und klicken Sie dann auf **Exportieren**. 2 Klicken Sie auf **OK**. Sie werden vom Browser gefragt, ob die Datei `sr<Server-Name>.zip` an den angegebenen Speicherort heruntergeladen werden soll. Wenn Sie einen Standardspeicherort für alle Browser-Downloads angegeben haben, wird die Datei möglicherweise automatisch dort gespeichert.
Importieren von ASSC-Schlüsseln	Importieren Sie von einem anderen McAfee ePO-Server exportierte ASSC-Schlüssel, um Agenten vom jeweiligen Server den Zugriff auf diesen McAfee ePO-Server zu ermöglichen. 1 Klicken Sie auf **Importieren**. 2 Wechseln Sie in den Speicherort, in dem Sie den Schlüssel gespeichert haben (in der Standardeinstellung auf dem Desktop), wählen Sie den Schlüssel aus, und klicken Sie dann auf **Öffnen**. 3 Klicken Sie auf **Weiter**, und überprüfen Sie die auf der Seite Schlüssel importieren angezeigten Informationen. 4 Klicken Sie auf **Speichern**.

Aktion	Vorgehensweise
Festlegen eines ASSC-Schlüsselpaars als Master	Geben Sie ein anderes Schlüsselpaar als Master an. Geben Sie nach dem Importieren oder Generieren eines neuen Schlüsselpaars einen Master-Schlüssel an. 1 Wählen Sie in der Liste **Schlüssel für sichere Agenten-Server-Kommunikation** einen Schlüssel aus, und klicken Sie dann auf **Als Master festlegen**. 2 Erstellen Sie für die Agenten einen Aktualisierungs-Task, der sofort ausgeführt wird, sodass die Agenten nach der nächsten Agent-Server-Kommunikation aktualisiert werden. Stellen Sie sicher, dass das Agenten-Schlüsselaktualisierungspaket im ePolicy Orchestrator-Master-Repository eingecheckt ist. Das neue Schlüsselpaar wird von Agenten verwendet, sobald der nächste Aktualisierungs-Task für McAfee Agent abgeschlossen ist. Sie können jederzeit sehen, von welchen Agenten ASSC-Schlüsselpaare in der Liste verwendet werden. 3 Sichern Sie alle Schlüssel.
Löschen von ASSC-Schlüsseln	Löschen Sie keine Schlüssel, die noch von Agenten verwendet werden. Andernfalls ist keine Kommunikation zwischen diesen Agenten und dem McAfee ePO-Server möglich. 1 Wählen Sie in der Liste **Schlüssel für sichere Agenten-Server-Kommunikation** den zu entfernenden Schlüssel aus, und klicken Sie dann auf **Löschen**. 2 Klicken Sie auf **OK**, um das Schlüsselpaar auf diesem Server zu löschen.

Anzeigen von Systemen, die ein ASSC-Schlüsselpaar verwenden

Sie können die Systeme anzeigen, deren Agenten ein bestimmtes ASSC-Schlüsselpaar aus der Liste **Schlüssel für sichere Agenten-Server-Kommunikation** verwenden.

Nachdem Sie ein bestimmtes Schlüsselpaar als Master festgelegt haben, möchten Sie eventuell die Systeme anzeigen, die noch das vorherige Schlüsselpaar verwenden. Löschen Sie ein Schlüsselpaar erst dann, wenn Sie wissen, dass es von keinem Agenten mehr verwendet wird.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste Einstellungskategorien den Eintrag **Sicherheitsschlüssel** aus, und klicken Sie dann auf **Bearbeiten**.

2 Wählen Sie in der Liste **Schlüssel für sichere Agenten-Server-Kommunikation** einen Schlüssel aus, und klicken Sie dann auf **Agenten anzeigen**.

Auf der Seite **Systeme, die diesen Schlüssel verwenden** sind alle Systeme aufgeführt, deren Agenten den ausgewählten Schlüssel verwenden.

Verwenden desselben ASSC-Schlüsselpaares für alle Server und Agenten

Vergewissern Sie sich, dass für alle McAfee ePO-Server und Agenten das gleiche Schlüsselpaar für sichere Agenten-Server-Kommunikation (ASSC) verwendet wird.

Wenn in der Umgebung eine größere Anzahl von verwalteten Systemen vorhanden ist, McAfee sollten Sie diesen Vorgang phasenweise durchführen, damit Sie Agenten-Aktualisierungen überwachen können.

Vorgehensweise

1 Erstellen Sie einen Agenten-Aktualisierungs-Task.

2 Exportieren Sie die ausgewählten Schlüssel vom ausgewählten McAfee ePO-Server.

3 Importieren Sie die exportierten Schlüssel auf allen anderen Servern.

4 Legen Sie den importierten Schlüssel auf allen Servern als Master fest.

5 Führen Sie zwei Agenten-Reaktivierungen aus.

6 Wenn von allen Agenten die neuen Schlüssel verwendet werden, können Sie die nicht mehr verwendeten Schlüssel löschen.

7 Sichern Sie alle Schlüssel.

Verwenden verschiedener ASSC-Schlüsselpaare für jeden McAfee ePO-Server

Sie können für jeden McAfee ePO-Server ein anderes ASSC-Schlüsselpaar verwenden, um sicherzustellen, dass alle Agenten mit den erforderlichen McAfee ePO-Servern in einer Umgebung kommunizieren können, in der jeder Server über ein eigenes, eindeutiges ASSC-Schlüsselpaar verfügen muss.

Agenten können nicht mit mehreren Servern gleichzeitig kommunizieren. Der McAfee ePO-Server kann mehrere Schlüssel besitzen, um mit verschiedenen Agenten zu kommunizieren, aber nicht umgekehrt. Agenten können nicht über mehrere Schlüssel verfügen, um mit mehreren McAfee ePO-Servern zu kommunizieren.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Exportieren Sie von jedem McAfee ePO-Server in Ihrer Umgebung das ASSC-Hauptschlüsselpaar in einen temporären Speicherort.

2 Importieren Sie jedes dieser Schlüsselpaare auf die einzelnen McAfee ePO-Server.

Sichern und Wiederherstellen von Schlüsseln

Sie sollten in regelmäßigen Abständen sämtliche Sicherheitsschlüssel sichern und stets eine Sicherung erstellen, bevor Sie Änderungen an den wichtigsten Verwaltungseinstellungen vornehmen.

Bewahren Sie die Sicherung in einem sicheren Speicherort im Netzwerk auf, sodass die Schlüssel leicht wiederhergestellt werden können, falls sie auf dem McAfee ePO-Server verloren gehen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste **Einstellungskategorien** den Eintrag **Sicherheitsschlüssel** aus, und klicken Sie dann auf **Bearbeiten**.

Die Seite **Sicherheitsschlüssel: Bearbeiten** wird angezeigt.

2 Wählen Sie eine der folgenden Aktionen aus.

Aktionen	Vorgehensweise
Sichern aller Sicherheitsschlüssel	**1** Klicken Sie im unteren Teil der Seite auf **Alle sichern**. Das Dialogfeld **Schlüsselspeicher sichern** wird angezeigt. **2** Sie können optional ein Kennwort zum Verschlüsseln der Schlüsselspeicher-ZIP-Datei eingeben oder auf **OK** klicken, um die Dateien in unverschlüsselter Textform zu speichern. **3** Klicken Sie im Dialogfeld **Dateidownload** auf **Speichern**, um eine ZIP-Datei mit allen Sicherheitsschlüsseln zu erstellen. Das Dialogfeld **Speichern unter** wird angezeigt. **4** Wechseln Sie zu einem sicheren Netzwerkspeicherort, in dem die ZIP-Datei gespeichert werden soll, und klicken Sie dann auf **Speichern**.
Wiederherstellen von Sicherheitsschlüsseln	**1** Klicken Sie unten auf der Seite auf **Alle wiederherstellen**. Die Seite **Sicherheitsschlüssel wiederherstellen** wird angezeigt. **2** Wechseln Sie zu der ZIP-Datei, in der sich die Sicherheitsschlüssel befinden, wählen Sie die Datei aus, und klicken Sie dann auf **Weiter**. Die Seite **Zusammenfassung** des Assistenten **Sicherheitsschlüssel wiederherstellen** wird angezeigt. **3** Wechseln Sie zu den Schlüsseln, mit denen Sie Ihre vorhandenen Schlüssel ersetzen möchten, und klicken Sie auf **Weiter**. **4** Klicken Sie auf **Wiederherstellen**. Die Seite **Sicherheitsschlüssel: Bearbeiten** wird erneut angezeigt. **5** Wechseln Sie zu einem sicheren Netzwerkspeicherort, in dem die ZIP-Datei gespeichert werden soll, und klicken Sie dann auf **Speichern**.
Wiederherstellen von Sicherheitsschlüsseln aus einer Sicherungsdatei	**1** Klicken Sie unten auf der Seite auf **Alle wiederherstellen**. Die Seite **Sicherheitsschlüssel wiederherstellen** wird angezeigt. **2** Wechseln Sie zu der ZIP-Datei, in der sich die Sicherheitsschlüssel befinden, wählen Sie die Datei aus, und klicken Sie dann auf **Weiter**. Die Seite **Zusammenfassung** des Assistenten **Sicherheitsschlüssel wiederherstellen** wird angezeigt. **3** Wechseln Sie zu der ZIP-Sicherungsdatei, wählen Sie sie aus, und klicken Sie anschließend auf **Weiter**. **4** Klicken Sie unten auf der Seite auf **Alle wiederherstellen**. Der Assistent **Sicherheitsschlüssel wiederherstellen** wird geöffnet. **5** Wechseln Sie zu der ZIP-Sicherungsdatei, wählen Sie sie aus, und klicken Sie anschließend auf **Weiter**. **6** Überprüfen Sie, ob die Schlüssel in dieser Datei mit denjenigen identisch sind, mit denen Sie die vorhandenen Schlüssel überschreiben möchten, und klicken Sie anschließend auf **Wiederherstellen**.

13 Software-Manager

Mit dem Software-Manager können Sie McAfee-Software sowie Software-Komponenten überprüfen und erwerben.

Inhalt

- *Inhalt des Software-Managers*
- *Einchecken, Aktualisieren und Entfernen von Software mit dem Software-Manager*
- *Überprüfen der Produktkompatibilität*

Inhalt des Software-Managers

Mit dem Software-Manager müssen Sie nicht mehr auf die McAfee-Website für den Produkt-Download zugreifen, um neue McAfee-Software und Software-Aktualisierungen zu erhalten.

Sie können mit dem Software-Manager Folgendes herunterladen:

- Lizenzierte Software
- Test-Software
- Software-Aktualisierungen
- Produktdokumentationen

DAT-Dateien und Scan-Module sind nicht über den Software-Manager erhältlich.

Lizenzierte Software

Lizenzierte Software ist jegliche Software, die Ihr Unternehmen von McAfee erworben hat. Im **Software-Manager** in der ePolicy Orchestrator-Konsole wird in der Produktkategorie **Nicht eingecheckte Software** jegliche Software angezeigt, für die Ihr Unternehmen eine Lizenz besitzt, die jedoch noch nicht auf dem Server installiert ist. Die neben jeder Unterkategorie in der Liste **Produktkategorien** angezeigte Zahl zeigt an, wie viele Produkte verfügbar sind.

Test-Software

Test-Software ist Software, für die Ihr Unternehmen gegenwärtig keine Lizenz besitzt. Sie können auf dem Server Test-Software installieren. Deren Funktionalität kann jedoch eingeschränkt sein, bis Sie eine Produktlizenz erwerben.

Software-Aktualisierungen

Wenn für die von Ihnen verwendete Software eine neue Aktualisierung veröffentlicht wird, können Sie den **Software-Manager** verwenden, um neue Pakete und Erweiterungen einzuchecken. Verfügbare Software-Aktualisierungen sind in der Kategorie **Aktualisierungen verfügbar** aufgeführt.

Produktdokumentationen

Neue und aktualisierte Produktdokumentationen können über den **Software-Manager** bezogen werden. Hilfeerweiterungen können automatisch installiert werden. Außerdem können über den **Software-Manager** auch PDF- und HTML-Dokumentationen (wie Produkthandbücher und Versionsinformationen) heruntergeladen werden.

Informationen zu Abhängigkeiten bei Software-Komponenten

Viele der Software-Produkte, die Sie zur Nutzung mit Ihrem McAfee ePO-Server installieren können, verfügen über vordefinierte Abhängigkeiten zu anderen Komponenten. Abhängige Elemente für Produkterweiterungen werden automatisch installiert. Für alle anderen Produktkomponenten müssen Sie die Liste der Abhängigkeiten auf der Seite **Komponentendetails** überprüfen und diese Komponenten dann vorher installieren.

Einchecken, Aktualisieren und Entfernen von Software mit dem Software-Manager

Im Software-Manager können Sie verwaltete Produktkomponenten auf Ihrem Server einchecken, aktualisieren und entfernen.

Im Software-Manager kann sowohl auf lizenzierte Software als auch auf Testversionen zugegriffen werden.

Welche Software verfügbar ist und ob sie sich in der Kategorie **Lizenziert** oder **Test** befindet, hängt von Ihrem Lizenzschlüssel ab. Weitere Informationen erhalten Sie von Ihrem Administrator.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Software** | **Software-Manager**.

2 Wählen Sie auf der Seite **Software-Manager** in der Liste **Produktkategorien** eine der folgenden Kategorien aus, oder suchen Sie Ihre Software mithilfe des Suchfelds:

- **Aktualisierungen verfügbar** – In dieser Kategorie sind alle verfügbaren Aktualisierungen für lizenzierte Software-Komponenten aufgeführt, die auf diesem McAfee ePO-Server bereits installiert oder eingecheckt sind.
- **Eingecheckte Software** – In dieser Kategorie wird sämtliche Software angezeigt (sowohl vom Typ **Lizenziert** als auch **Test**), die auf diesem Server installiert oder eingecheckt ist.

  Wenn eine kürzlich für ein Produkt hinzugefügte Lizenz als **Test** aufgeführt ist, klicken Sie auf **Aktualisieren**, damit der Wert bei Lizenziert aktualisiert und das Produkt unter **Eingecheckte Software** als **Lizenziert** geführt wird.

- **Nicht eingecheckte Software** – In dieser Kategorie wird Software aufgeführt, die verfügbar, auf diesem Server jedoch nicht installiert ist.
- **Software (nach Beschriftung)** – In dieser Kategorie ist Software nach ihrer Funktion laut Beschreibung von McAfee-Produkt-Suites aufgeführt.

3 Wenn Sie die richtige Software gefunden haben, klicken Sie auf eine der folgenden Optionen:

- **Herunterladen**, um die Produktdokumentation in einen Speicherort in Ihrem Netzwerk herunterzuladen.
- **Einchecken**, um eine Produkterweiterung oder ein Paket auf diesem Server einzuchecken.

- **Aktualisieren**, um ein Paket oder eine Erweiterung zu aktualisieren, das bzw. die derzeit auf diesem Server installiert oder eingecheckt ist.
- **Entfernen**, um ein Paket oder eine Erweiterung zu deinstallieren, das bzw. die derzeit auf diesem Server installiert oder eingecheckt ist.

4 Lesen Sie auf der Seite **Zusammenfassung zum Einchecken der Software** die Produktdetails und den Endbenutzer-Lizenzvertrag (EULA) durch, akzeptieren Sie ihn, und klicken Sie dann auf **OK**, um den Vorgang abzuschließen.

Überprüfen der Produktkompatibilität

Sie können eine Produktkompatibilitätsüberprüfung konfigurieren, um automatisch eine Produktkompatibilitätsliste von McAfee herunterzuladen.

In dieser Liste sind Produkte aufgeführt, die in Ihrer McAfee ePO-Umgebung nicht mehr kompatibel sind.

Diese Überprüfung wird in McAfee ePO jedes Mal durchgeführt, wenn die Installation und der Start einer Erweiterung zu einem unerwünschten Zustand Ihres Servers führen könnten. Diese Überprüfung findet in den folgenden Szenarien statt:

- Während eines Upgrades von einer früheren Version von McAfee ePO
- Wenn eine Erweiterung über das Menü **Erweiterungen** installiert wird.
- Bevor eine neue Erweiterung vom **Software-Manager** abgerufen wird
- Bei Empfang einer neuen Kompatibilitätsliste von McAfee
- Bei Ausführung des Tools zur Datenmigration

Details hierzu finden Sie im *McAfee ePolicy Orchestrator-Installationshandbuch*.

Produktkompatibilitätsüberprüfung

Bei der Produktkompatibilitätsüberprüfung wird anhand einer als Produktkompatibilitätsliste bezeichneten XML-Datei festgestellt, welche Produkterweiterungen mit einer Version von McAfee ePO *nicht kompatibel* sind.

Eine erste Liste ist bereits in dem McAfee ePO-Paket enthalten, das Sie von der McAfee-Website heruntergeladen haben. Beim Setup während einer Installation oder eines Upgrades wird für McAfee ePO automatisch eine aktuelle Liste der kompatiblen Erweiterungen aus einer vertrauenswürdigen McAfee-Quelle heruntergeladen. Wenn die Internetquelle nicht verfügbar ist oder die Liste nicht verifiziert werden kann, wird die letzte gespeicherte Version für McAfee ePO verwendet.

Die Produktkompatibilitätsliste wird einmal täglich vom McAfee ePO-Server im Hintergrund aktualisiert.

Fehlerbehebung

Wenn Sie die Liste der inkompatiblen Erweiterungen über das Installationsprogramm oder das Upgrade-Kompatibilitätsprogramm anzeigen und eine bekannte Ersatzerweiterung verfügbar ist, werden Sie benachrichtigt.

In einigen Fällen kann während eines Upgrades eine der folgenden Situationen auftreten:

- Eine Erweiterung blockiert das Upgrade und muss entfernt oder ersetzt werden, bevor das Upgrade fortgesetzt werden kann.
- Eine Erweiterung ist deaktiviert und muss nach Abschluss des McAfee ePO-Upgrades aktualisiert werden.

Ausführlichere Informationen dazu finden Sie unter *Blockierte oder deaktivierte Erweiterungen*.

Deaktivieren der automatischen Aktualisierungen

Sie können die automatischen Aktualisierungen der Produktkompatibilitätsliste deaktivieren, um zu verhindern, dass eine neue Liste heruntergeladen wird.

Der Download erfolgt im Hintergrund oder beim Aktualisieren von Inhalten des Software-Managers. Diese Einstellung ist hilfreich, wenn Ihr McAfee ePO-Server nicht über Internetzugriff für Datenempfang verfügt. Ausführliche Informationen dazu finden Sie unter *Ändern der Einstellungen für den Download der Produktkompatibilitätsliste*.

Wenn Sie die Einstellung für den Download der Produktkompatibilitätsliste erneut aktivieren, werden auch die automatischen Aktualisierungen der Produktkompatibilitätsliste im Software-Manager wieder aktiviert.

Verwenden einer manuell heruntergeladenen Produktkompatibilitätsliste

Eine manuell heruntergeladene Produktkompatibilitätsliste können Sie zum Beispiel dann verwenden, wenn Ihr McAfee ePO-Server nicht über Internetzugriff verfügt.

Die Liste können Sie bei den folgenden Gelegenheiten manuell herunterladen:

- Wenn Sie McAfee ePO installieren. Ausführliche Informationen dazu finden Sie unter *Blockierte oder deaktivierte Erweiterungen*.
- Wenn Sie über **Server-Einstellungen** | **Produktkompatibilitätsliste** eine Produktkompatibilitätsliste manuell hochladen. Diese Liste ist dann sofort nach dem Hochladen gültig.

Deaktivieren Sie die automatische Aktualisierung der Liste, um zu verhindern, dass die manuell heruntergeladene Produktkompatibilitätsliste überschrieben wird. Ausführliche Informationen dazu finden Sie unter *Ändern der Einstellungen für den Download der Produktkompatibilitätsliste*.

Klicken Sie auf ProductCompatibilityList.xml, um die Liste manuell herunterzuladen.

Blockierte oder deaktivierte Erweiterungen

Wenn eine Erweiterung in der Produktkompatibilitätsliste blockiert ist, wird das Software-Upgrade von McAfee ePO verhindert. Wenn eine Erweiterung deaktiviert ist, wird das Upgrade dadurch nicht blockiert. Die Erweiterung wird nach Abschluss des Upgrades jedoch erst aktiviert, wenn eine bekannte Ersatzerweiterung installiert wurde.

Befehlszeilenoptionen für die Installation der Produktkompatibilitätsliste

Mithilfe der folgenden Befehlszeilenoptionen für den Befehl `setup.exe` können Sie Downloads der Produktkompatibilitätsliste konfigurieren.

Befehl	Beschreibung
`setup.exe DISABLEPRODCOMPATUPDATE=1`	Deaktiviert das automatische Herunterladen der Produktkompatibilitätsliste von der McAfee-Website.
`setup.exe PRODCOMPATXML=<vollständiger_Dateiname_inklusive_Pfad>`	Gibt eine alternative Datei der Produktkompatibilitätsliste an.

Beide Befehlszeilenoptionen können gemeinsam in einer Befehlszeichenfolge verwendet werden.

Ändern der Einstellungen für den Download der Produktkompatibilitätsliste

Sie können die Produktkompatibilitätsliste entweder aus dem Internet herunterladen oder eine manuell heruntergeladene Liste verwenden, um Produkte zu ermitteln, die in Ihrer ePolicy Orchestrator-Umgebung nicht mehr kompatibel sind.

Bevor Sie beginnen

Als manuell heruntergeladene Produktkompatibilitätslisten sind nur gültige XML-Dateien von McAfee zulässig.

Falls Sie in der XML-Datei der Produktkompatibilitätsliste Änderungen vornehmen, wird die Datei ungültig.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste **Einstellungskategorien** den Eintrag **Produktkompatibilitätsliste** aus, und klicken Sie dann auf **Bearbeiten**.

   Eine Seite wird angezeigt, auf der die deaktivierten nicht kompatiblen Erweiterungen in einer Tabelle aufgelistet sind.

2. Klicken Sie auf **Deaktiviert**, um den automatischen und regelmäßigen Download der Produktkompatibilitätsliste von McAfee zu stoppen.

3. Klicken Sie auf **Durchsuchen**, wechseln Sie zu **Produktkompatibilitätsliste hochladen**, und klicken Sie dann auf **Speichern**.

Nachdem Sie den automatischen Download der Produktkompatibilitätsliste deaktiviert haben, verwendet Ihr McAfee ePO-Server so lange die gleiche Liste, bis Sie eine neue Liste hochladen oder den Server mit dem Internet verbinden und das automatische Herunterladen wieder aktivieren.

14 Produktausbringung

Mit ePolicy Orchestrator wird die Bereitstellung von Sicherheitsprodukten auf den verwalteten Systemen in einem Netzwerk vereinfacht, indem eine Benutzeroberfläche bereitgestellt wird, in der Bereitstellungen konfiguriert und geplant werden können.

Zum Bereitstellen von Produkten mittels ePolicy Orchestrator können Sie nach zwei Methoden vorgehen:

- Produktausbringungsprojekte, mit denen Sie den Ausbringungsprozess optimieren und zusätzliche Funktionen bereitstellen können
- Individuell erstellte und verwaltete Client-Task-Objekte und Tasks

Inhalt

- *Auswählen einer Methode zur Produktausbringung*
- *Vorteile von Produktausbringungsprojekten*
- *Erklärung der Seite Produktausbringung*
- *Anzeigen von Audit-Protokollen zu Produktausbringungen*
- *Anzeigen der Produktausbringung*
- *Ausbringen von Produkten mithilfe eines Ausbringungsprojekts*
- *Überwachen und Bearbeiten von Ausbringungsprojekten*
- *Beispiel für die Bereitstellung eines neuen Produkts*
- *Globale Aktualisierung*
- *Automatisches Ausbringen von Aktualisierungspaketen per globaler Aktualisierung*

Auswählen einer Methode zur Produktausbringung

Welche Methode zur Produktausbringung für Sie am besten geeignet ist, hängt von der bereits vorhandenen Konfiguration ab.

Produktausbringungsprojekte zeichnen sich durch einen vereinfachten Workflow sowie umfangreichere Funktionen zur Ausbringung auf Systemen aus, die von ePolicy Orchestrator verwaltet werden. Allerdings können **Produktausbringungsprojekte** nicht in Kombination mit oder zum Verwalten von Client-Task-Objekten und Tasks verwendet werden, die mit einer älteren Software als Version 5.0 erstellt wurden.

Wenn Sie Client-Tasks und Objekte, die außerhalb eines **Produktausbringungsprojekts** erstellt wurden, beibehalten und weiter nutzen möchten, müssen Sie die Client-Task-Objektbibliothek und die Zuweisungsschnittstellen verwenden. Sie können die vorhandenen Tasks und Objekte behalten, während Sie neue Ausbringungen mithilfe der Schnittstelle für **Produktausbringungsprojekte** erstellen.

Vorteile von Produktausbringungsprojekten

Produktausbringungsprojekte vereinfachen die Ausbringung von Sicherheitsprodukten auf verwalteten Systemen, da sie den für die Planung und Wartung von Ausbringungen im Netzwerk erforderlichen Zeit- und Verwaltungsaufwand verringern.

Indem bei Produktbereitstellungsprojekten viele der Schritte zusammengefasst werden, die zum Erstellen und Verwalten der einzelnen Produktbereitstellungs-Tasks erforderlich sind, wird der Bereitstellungsvorgang erheblich vereinfacht. Darüber hinaus ermöglichen diese Projekte folgende Aufgaben:

- **Ausführen einer Ausbringung auf beliebig vielen Systemen.** Sie können Ausbringungsprojekte so konfigurieren, dass Produkte auf neu hinzugefügten Systemen automatisch ausgebracht werden, wenn diese neuen Systeme mit den von Ihnen festgelegten Kriterien übereinstimmen.
- **Anhalten einer laufenden Ausbringung.** Sie haben nun die Möglichkeit, eine bereits begonnene Ausbringung bei Bedarf anzuhalten. Anschließend können Sie die Ausbringung zu jedem gewünschten Zeitpunkt wieder fortsetzen.
- **Deinstallieren eines zuvor bereitgestellten Produkts**: Wenn Sie nach Abschluss eines Bereitstellungsprojekts das entsprechende Produkt auf den Ihrem Projekt zugewiesenen Systemen deinstallieren möchten, wählen Sie in der Liste **Aktion** die Option Deinstallieren aus.

In der folgenden Tabelle werden die beiden Methoden zur Ausbringung von Produkten, d. h. einzelne Client-Task-Objekte und Produktausbringungsprojekte, miteinander verglichen.

Tabelle 14-1 Vergleich der Methoden zur Produktausbringung

Client-Task-Objekte	Vergleich der Funktionen	Produktausbringungsprojekt
Name und Beschreibung	Identisch	Name und Beschreibung
Erfassung von auszubringender Produkt-Software	Identisch	Erfassung von auszubringender Produkt-Software
Verwendung von Tags zur Auswahl von Zielsystemen	Verbessert in Produktbereitstellungsprojekten	Auswahl während der Bereitstellung: • **Beliebig viele**: Bei Bereitstellungen vom Typ Beliebig viele werden Systemstrukturgruppen oder Tags verwendet. Dadurch können Sie Systeme in bestimmte Gruppen verschieben oder Systemen bestimmte Tags zuweisen, sodass die Bereitstellung dann auf den entsprechenden Systemen durchgeführt wird. • **Festgelegt**: Bei Bereitstellungen vom Typ Festgelegt wird eine festgelegte bzw. definierte Auswahl an Systemen verwendet. Die Auswahl der Systeme erfolgt in der Systemstruktur oder mithilfe von Ausgabetabellen für Abfragen vom Typ Verwaltete Systeme.
Planung der Ausbringung	Ähnlich	Dank einer vereinfachten Ausbringungsplanung können Sie Ausbringungen entweder sofort oder zu einem geplanten Zeitpunkt ausführen.

Tabelle 14-1 Vergleich der Methoden zur Produktausbringung *(Fortsetzung)*

Client-Task-Objekte	Vergleich der Funktionen	Produktausbringungsprojekt
Nicht verfügbar	Neu in Produktausbringungsprojekten	Sie können den aktuellen Ausbringungsstatus überwachen (z. B. Ausbringungen, die geplant, aber noch nicht gestartet wurden, oder die gerade durchgeführt werden, angehalten oder abgeschlossen sind).
Nicht verfügbar	Neu in Produktbereitstellungsprojekten	Sie können einen Verlaufs-Snapshot zu Daten über die Anzahl der Systeme anzeigen, auf denen die Bereitstellung erfolgt. Nur bei Bereitstellungen vom Typ Festgelegt.
Nicht verfügbar	Neu in Produktausbringungsprojekten	Sie können den Status einzelner Systemausbringungen anzeigen (z. B. Installiert, Ausstehend oder Fehlgeschlagen).
Nicht verfügbar	Neu in Produktbereitstellungsprojekten	Sie können eine vorhandene Bereitstellungszuweisung mithilfe folgender Optionen ändern: • Neu erstellen zum Ändern einer vorhandenen Bereitstellung • Bearbeiten • Duplizieren • Löschen • Anhalten und Anhalten einer Bereitstellung • Weiter und Fortsetzen einer Bereitstellung • Deinstallieren

Erklärung der Seite Produktausbringung

Die Seite Produktausbringung ist die zentrale Stelle, an der Sie Produktausbringungsprojekte erstellen, überwachen und verwalten können.

Die Seite ist in zwei Hauptbereiche aufgeteilt (Bereich 1 und 2 im Bild unten), wobei der zweite Bereich noch einmal in fünf kleinere Bereiche unterteilt ist.

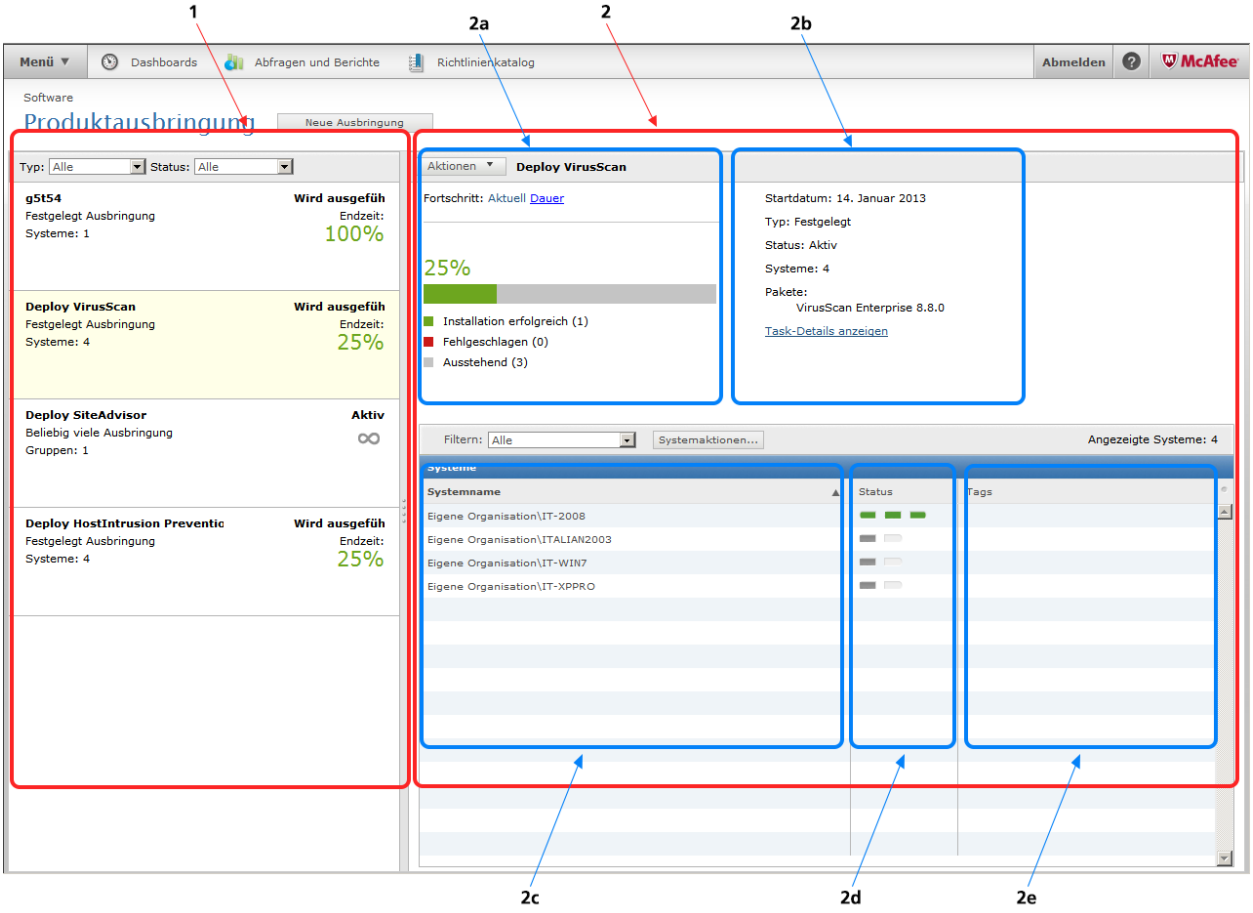


Abbildung 14-1 Produktausbringung, Seite

Bei den beiden Hauptbereichen handelt es sich um:

1 *Ausbringungszusammenfassung* – Hier sind die Produktausbringungen aufgelistet, die Sie nach Typ und Status filtern können. Darüber hinaus erhalten Sie einen schnellen Überblick über deren Fortschritt. Wenn Sie auf eine Ausbringung klicken, werden deren Details im Bereich mit den Ausbringungsdetails angezeigt.

> Ein Ausrufezeichen bedeutet, dass die Ausbringung entweder gerade deinstalliert wird oder dass das von der Ausbringung verwendete Paket verschoben oder gelöscht wurde.

2 *Bereitstellungsdetails*: Hier werden die Einzelheiten zu der ausgewählten Bereitstellung aufgelistet. Dieser Bereich enthält folgende Unterbereiche:

2a *Statusmonitor*: Welche Fortschritts- und Statusinformationen im Einzelnen angezeigt werden, hängt vom Typ der Bereitstellung und deren Status ab:

- Bei Ausbringungen für eine beliebige Anzahl an Systemen wird ein Kalender angezeigt, wenn die Ausbringung noch aussteht, oder ein Balkendiagramm, wenn die Ausbringung gerade durchgeführt wird.
- Bei Ausbringungen für eine festgelegte Auswahl an Systemen wird ein Kalender angezeigt, wenn die Ausbringung noch aussteht, ein Balkendiagramm, wenn **Aktuell** ausgewählt ist, bzw. ein Histogramm, wenn **Dauer** ausgewählt ist.

Sie können eine Bereitstellung über Aktion ändern.

2b *Details*: In diesem Bereich werden Details zur Konfiguration und zum Status der Bereitstellung angezeigt. Bei Bedarf können Sie auf **Task-Details anzeigen** klicken, um die Seite Bereitstellung bearbeiten zu öffnen.

2c **Systemname**: Hier wird eine filterbare Liste der Zielsysteme angezeigt, die die Bereitstellung erhalten. Welche Systeme angezeigt werden, richtet sich nach dem Typ der Bereitstellung sowie danach, auf welche Weise die Systeme ausgewählt wurden (d. h. einzeln, per Tags, per Systemstrukturgruppen oder mithilfe von Abfragetabellen).

Wenn Sie auf **Systemaktionen** klicken, wird die gefilterte Liste der Systeme in einem Dialogfeld angezeigt, das weitere Details enthält und in dem Sie Aktionen (wie Aktualisierungen oder Reaktivierungen) an den Systemen durchführen können.

2d **Status** – Zeigt eine dreiteilige Statusleiste an, die den Fortschritt der Ausbringung und deren Status angibt.

2e **Tags** – Hier werden die den Systemen zugeordneten Tags angezeigt.

Anzeigen von Audit-Protokollen zu Produktausbringungen

In den Audit-Protokolle der Ausbringungsprojekte sind alle Produktausbringungen aufgezeichnet, die über die Konsole mithilfe der Funktion zur Produktausbringung durchgeführt wurden.

Diese Audit-Protokolleinträge werden auf der Seite **Produktausbringung** im Bereich mit den Ausbringungsdetails in einer sortierbaren Tabelle sowie auf der Seite **Audit-Protokoll** angezeigt, die Protokolleinträge von allen überwachbaren Benutzeraktionen enthält. Mithilfe dieser Protokolle können Sie Produktausbringungen überwachen, erstellen, bearbeiten, duplizieren, löschen und deinstallieren. Klicken Sie auf einen Protokolleintrag, um dessen Details anzuzeigen.

Anzeigen der Produktausbringung

Bei der ersten Produktausbringung wird in ePolicy Orchestrator automatisch eine Produktausbringung erstellt. Diese Produktausbringung können Sie als Grundlage verwenden, um weitere Produktausbringungen zu erstellen.

Bevor Sie beginnen

Es sind keine Standard-Produktbereitstellungen vorhanden. Sie müssen Erste Schritte ausführen, um eine Produktbereitstellung zu erstellen.

Detaillierte Informationen zur Produktausbringung finden Sie unter *Produktausbringung*.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wenn Sie die erste Produktbereitstellung anzeigen möchten, wählen Sie **Menü** | **Produktbereitstellung** aus.

Für die erste erstellte Produktbereitstellung wird der Name der **Systemstruktur**gruppe verwendet, die Sie in Erste Schritte erstellt haben. Sie wird in der Liste **Übersicht über Bereitstellung** als Eigene Gruppe der ersten Bereitstellung angezeigt. Beispiel: "Eigene Gruppe der ersten Bereitstellung".

2 Wenn Sie Details zur Produktbereitstellung anzeigen möchten, wählen Sie den Namen der Produktbereitstellung aus, den Sie in der URL-Adresse für die erste Produktbereitstellung zugewiesen haben. Auf der Seite werden nun die Details der Produktbereitstellungskonfiguration angezeigt.

Ändern Sie diese Standard-Produktbereitstellung nicht. Diese Bereitstellung wird täglich ausgeführt, um die verwalteten Systeme zu aktualisieren, falls eine Aktualisierung für eines der Produkte oder McAfee Agent verfügbar ist.

Sie haben nun alle nötigen Informationen zum Speicherort und zur Konfiguration der ersten Produktbereitstellung. Sie können diese Produktbereitstellung auch duplizieren, um zum Beispiel **McAfee Agent** auf Plattformen mit anderen Betriebssystemen bereitzustellen.

Sie können außerdem den zuerst erstellten Client-Task mit beispielsweise dem Namen Eigene Gruppe der ersten Bereitstellung ändern. Sie finden den Client-Task, indem Sie auf **Menü** | **Client-Task-Katalog** klicken. Er ist bei den Client-Task-Typen unter Produktbereitstellung aufgelistet.

Ausbringen von Produkten mithilfe eines Ausbringungsprojekts

Wenn Sie Sicherheitsprodukte mithilfe eines Produktausbringungsprojekts auf verwalteten Systemen ausbringen, können Sie die auszubringenden Produkte sowie die Zielsysteme ganz leicht auswählen und die Ausbringung einfach planen.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Software** | **Produktausbringung**.

2 Klicken Sie auf **Neue Ausbringung**, um die Seite **Neue Ausbringung** zu öffnen und ein neues Projekt zu starten.

3 Geben Sie einen Namen und eine Beschreibung für die Ausbringung ein. Nach dem Speichern der Ausbringung wird dieser Name auf der Seite **Produktausbringung** angezeigt.

4 Bereitstellungstyp auswählen:

- **Beliebig viele**: Die Systeme, die diese Ausbringung erhalten, werden mithilfe von Systemstrukturgruppen oder Tags konfiguriert. Dadurch können Sie im Laufe der Zeit ändern, welche Systeme eine Ausbringung erhalten, indem Sie die gewünschten Systeme den jeweiligen Gruppen oder Tags hinzufügen bzw. daraus entfernen.
- **Festgelegt**: Hierbei wird eine feste bzw. definierte Auswahl an Systemen verwendet, die die Ausbringung erhalten sollen. Die Auswahl der Systeme erfolgt in der Systemstruktur oder mithilfe von Ausgabetabellen für Abfragen vom Typ **Verwaltete Systeme**.

Wenn die Sicherheitsprodukte automatisch aktualisiert werden sollen, wählen Sie **Automatische Aktualisierung** aus. Damit werden auch die HotFixes und Patches für das Produkt automatisch bereitgestellt.

Wenn Sie **Automatische Aktualisierung** ausgewählt haben, können Sie das Produkt nicht deinstallieren.

5 Wählen Sie zum Angeben der auszubringenden Software ein Produkt in der Liste **Paket** aus. Klicken Sie zum Hinzufügen oder Entfernen von Paketen auf **+** bzw. **-**.

Damit Software ausgebracht werden kann, muss sie im Master-Repository eingecheckt sein. Die Felder **Sprache** und **Zweig** werden anhand der im Master-Repository angegebenen Informationen zu Sprache und Speicherort automatisch ausgefüllt.

6 Im Textfeld **Befehlszeile** können Sie Optionen für befehlszeilengestützte Installationen angeben. Informationen über Befehlszeilenoptionen finden Sie in der Produktdokumentation der jeweiligen auszubringenden Software.

7 Klicken Sie im Abschnitt **Systeme auswählen** auf **Systeme auswählen**, um das Dialogfeld **Systemauswahl** zu öffnen.

Das Dialogfeld **Systemauswahl** ist ein Filter, mit dem Sie Gruppen in der Systemstruktur, Tags oder eine Untermenge gruppierter oder gekennzeichneter Systeme auswählen können. Die auf den einzelnen Registerkarten dieses Dialogfelds ausgewählten Elemente werden verkettet, um den kompletten Satz an Zielsystemen für die Bereitstellung zu filtern.

Wenn die Systemstruktur beispielsweise eine "Gruppe A" enthält, in der sich sowohl Server als auch Workstations befinden, können Sie die gesamte Gruppe, nur die Server oder Workstations (wenn diese mit den entsprechenden Tags gekennzeichnet sind) oder eine Untermenge der Systemtypen in "Gruppe A" herausfiltern.

Bei festgelegten Bereitstellungen ist die Zahl der Systeme, die eine Bereitstellung erhalten, auf maximal 500 beschränkt.

Konfigurieren Sie bei Bedarf folgende Optionen:

- **Bei jeder Richtlinienerzwingung ausführen (nur Windows)**
- **Aufschieben der Ausbringung durch Endbenutzer zulassen (nur Windows)**
- **Maximal zulässige Anzahl von Aufschubvorgängen**
- **Option zum Aufschieben läuft ab nach**
- **Diesen Text anzeigen**

8 Wählen Sie eine Startzeit oder einen Plan für die Bereitstellung aus:

- **Sofort ausführen** – Startet den Ausbringungs-Task während des nächsten ASKIs.
- **Einmal** – Öffnet den Planer, in dem Sie das Startdatum, die Uhrzeit und ein Zufallsintervall konfigurieren können.

9 Klicken Sie nach Abschluss aller Einstellungen oben auf der Seite auf **Speichern**. Die Seite **Produktausbringung** wird geöffnet, auf der Ihr neues Projekt zur Liste der Ausbringungen hinzugefügt ist.

Nachdem Sie ein Ausbringungsprojekt erstellt haben, wird automatisch ein Client-Task mit den Ausbringungseinstellungen erstellt.

Überwachen und Bearbeiten von Ausbringungsprojekten

Auf der Seite Produktbereitstellung können Sie Bereitstellungsprojekte erstellen, verfolgen und ändern.

In der folgenden Anleitung wird in den ersten Schritten beschrieben, wie Sie ein vorhandenes Ausbringungsprojekt mithilfe der Benutzeroberfläche auswählen und überwachen können, während in den letzten Schritten erläutert wird, wie Sie dieses Ausbringungsprojekt durch Auswahl von Aktionen ändern können.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Software** | **Produktbereitstellung**. Die Seite Produktbereitstellung wird angezeigt.

2 Filtern Sie die Liste der Bereitstellungsprojekte nach einer oder beiden der folgenden Optionen:

- **Typ**: Filtert die anzuzeigenden Bereitstellungen nach Alle, Beliebig viele oder Festgelegt.
- **Status**: Filtert die anzuzeigenden Bereitstellungen nach Alle, Fertig gestellt, Wird ausgeführt, Ausstehend, Aktiv oder Angehalten.

3 Wenn Sie links auf der Seite auf eine Bereitstellung in der Liste klicken, werden rechts die Details zu dieser Bereitstellung angezeigt.

4 Im Abschnitt Fortschritt der Detailanzeige können Sie Folgendes anzeigen:

- Einen Kalender mit dem Startdatum für ausstehende Ausbringungen auf beliebig vielen oder auf einer festgelegten Auswahl von Systemen.
- Ein Histogramm mit Systemen und der Zeitdauer bis zum Abschluss für Ausbringungen auf einer festgelegten Auswahl von Systemen.
- Eine Statusleiste, die den Fortschritt von Systemausbringungen und -deinstallationen anzeigt.

5 Klicken Sie auf **Aktion**, und wählen Sie eine der folgenden Optionen aus, um eine Bereitstellung zu ändern:

- **Bearbeiten**
- **Löschen**
- **Duplizieren**
- **Als fertig gestellt kennzeichnen**
- **Fortsetzen**
- **Anhalten**
- **Deinstallieren**

6 Klicken Sie im Detailbereich auf **Task-Details anzeigen**, um die Seite Ausbringung bearbeiten zu öffnen, auf der Sie die Einstellungen für die Ausbringung anzeigen und ändern können.

7 Klicken Sie in der Tabelle Systeme auf eine der folgenden Optionen in der Liste **Filter**, um den Typ der angezeigten Systeme zu ändern:

Welche Optionen in der Liste aufgeführt sind, hängt vom aktuellen Status der Bereitstellung ab.

- Für die Aktion Deinstallieren sind die folgenden Filter verfügbar: **Alle**, **Entfernte Pakete**, **Ausstehend** und **Fehlgeschlagen**
- Bei allen anderen Aktionen sind die folgenden Filter verfügbar: **Alle**, **Installation erfolgreich**, **Ausstehend** und **Fehlgeschlagen**

8 In der Tabelle **Systeme** können Sie folgende Aktionen durchführen:

- In der Spalte Status können Sie den Status der aufgelisteten Zielsysteme überprüfen. Der Fortschritt der Bereitstellung wird in einer dreiteiligen Statusleiste angezeigt.
- In der Spalte Tags können Sie die den einzelnen Zielsystemen zugeordneten Tags überprüfen.
- Wenn Sie auf **Systemaktionen** klicken, können Sie die Liste der Systeme auf einer neuen Seite anzeigen, auf der Sie an den ausgewählten Systemen systemspezifische Aktionen durchführen können.

Beispiel für die Bereitstellung eines neuen Produkts

Nach der McAfee ePO-Installation und der ersten Produktausbringung müssen Sie alle weiteren Produktausbringungen mit einem Projekt für die Produktausbringung oder manuell mit einem Client-Task-Objekt erstellen.

In diesem Beispiel werden Sie durch die Erstellung eines Produktausbringungsprojekts für McAfee VirusScan Enterprise geführt.

Vorgehensweise

1 Wählen Sie **Menü** | **Software** | **Produktausbringung**aus, und klicken Sie dann auf **Neue Ausbringung**.

2 Konfigurieren Sie auf der Seite Neue Ausbringung die folgenden Einstellungen.

Option	Beschreibung
Name und **Beschreibung**	Geben Sie einen Namen und eine Beschreibung für die Ausbringung ein. Nach dem Speichern der Ausbringung wird dieser Name auf der Seite Ausbringung angezeigt.
Typ	Wählen Sie in der Liste die Option **Beliebig viele** aus. Die Systeme, die diese Ausbringung erhalten, werden mithilfe von Systemstrukturgruppen oder Tags konfiguriert. Wenn Sie diesen Typ auswählen, können Sie im Lauf der Zeit ändern, welche Systeme eine Ausbringung erhalten, indem Sie die gewünschten Systeme zu den jeweiligen Gruppen oder Tags hinzufügen bzw. daraus entfernen. Zum automatischen Aktualisieren von Sicherheitsprodukten wählen Sie **Automatische Aktualisierung** aus. Mit dieser Funktion werden auch die HotFixes und Patches für das Produkt automatisch bereitgestellt. Wenn Sie **Automatische Aktualisierung** ausgewählt haben, können Sie das Produkt nicht deinstallieren.
Paket	Wählen Sie in der Liste die Option **VirusScan Enterprise** aus.
Sprache und **Zweig**	Wählen Sie Sprache und Zweig aus, wenn Sie nicht die Standardeinstellungen verwenden möchten.
Befehlszeile	Im Textfeld können Sie Optionen für befehlszeilengestützte Installationen angeben. Details hierzu finden Sie im *McAfee VirusScan Enterprise-Installationshandbuch*.

Option	Beschreibung
Systeme auswählen	Klicken Sie auf **Systeme auswählen**, um das Dialogfeld Systemauswahl zu öffnen. Das Dialogfeld Systemauswahl ist ein Filter, mit dem Sie Gruppen in der Systemstruktur, Tags oder eine Untermenge gruppierter oder gekennzeichneter Systeme auswählen können. Die auf den einzelnen Registerkarten dieses Dialogfelds ausgewählten Elemente werden verkettet, um den kompletten Satz an Zielsystemen für die Ausbringung zu filtern. Konfigurieren Sie bei Bedarf folgende Optionen: • **Bei jeder Richtlinienerzwingung ausführen (nur Windows)** • **Aufschieben der Ausbringung durch Endbenutzer zulassen (nur Windows)** • **Maximal zulässige Anzahl von Aufschubvorgängen** • **Option zum Aufschieben läuft ab nach** • **Diesen Text anzeigen**
Startzeit auswählen	Wählen Sie eine Startzeit oder einen Plan für die Ausbringung aus: • **Sofort ausführen**: Startet den Ausbringungs-Task nach dem nächsten ASKI. • **Einmal**: Öffnet den Planer, in dem Sie das Startdatum, die Uhrzeit und den Zufallsgenerator konfigurieren können.
Speichern	Klicken Sie nach Abschluss aller Einstellungen oben auf der Seite auf **Speichern**. Die Seite **Produktausbringung** wird geöffnet, auf der das neue Projekt zur Liste der Ausbringungen hinzugefügt ist.

Nachdem Sie ein Ausbringungsprojekt erstellt haben, wird automatisch ein Client-Task mit den Ausbringungseinstellungen erstellt.

3 Vergewissern Sie sich auf der Seite Produktausbringung, dass das Produktausbringungsprojekt richtig funktioniert, indem Sie die folgenden Informationen überprüfen.

Option	Beschreibung
Übersicht über Ausbringung	Klicken Sie auf das Produktausbringungsprojekt, das Sie im vorherigen Schritt erstellt haben. Auf der rechten Seite werden die Details angezeigt. Da es sich um eine Ausbringung für beliebig viele Systeme handelt, wird das Unendlichkeitssymbol ∞ unter Wird ausgeführt angezeigt.
Ausbringungsdetails	Hier haben Sie folgende Möglichkeiten: • Klicken Sie auf **Aktionen**, um die ausgewählte Ausbringung zu ändern. • Zeigen Sie **Fortschritt**, **Status** und **Details** der ausgewählten Ausbringung an. • Zeigen Sie die **Systeme**, **Systemaktionen**, **Status** und **Tags** an, die der ausgewählten Ausbringung zugeordnet sind.

Globale Aktualisierung

Durch die globale Aktualisierung wird die Replikation an die verteilten Repositories automatisiert, und die verwalteten Systeme werden auf dem aktuellen Stand gehalten.

Es sind keine Replikations- und Aktualisierungs-Tasks erforderlich. Stattdessen wird durch das Einchecken von Inhalten in das Master-Repository eine globale Aktualisierung ausgelöst. Der gesamte Vorgang nimmt in den meisten Umgebungen nicht mehr als eine Stunde in Anspruch.

Sie können außerdem angeben, durch welche Pakete und Aktualisierungen eine globale Aktualisierung ausgelöst wird. Wenn nur bestimmte Inhalte eine globale Aktualisierung auslösen sollen, müssen Sie einen Replikations-Task erstellen, mit dem alle anderen Inhalte verteilt werden.

Wenn Sie die globale Aktualisierung verwenden, empfiehlt McAfee, einen regelmäßigen Abruf-Task (zum Aktualisieren des Master-Repositorys) für einen Zeitpunkt mit geringem Netzwerkverkehr zu planen. Die globale Aktualisierung ist zwar die schnellste Aktualisierungsmethode, verursacht jedoch verstärkten Netzwerkverkehr.

Die globale Aktualisierung

1. Die Inhalte werden in das Master-Repository eingecheckt.
2. Der Server führt eine inkrementelle Replizierung in alle verteilten Repositories durch.
3. Vom Server wird eine SuperAgent-Reaktivierung für alle SuperAgents in der Umgebung ausgegeben.
4. Vom SuperAgent wird eine Nachricht über die globale Aktualisierung an alle Agenten in dem SuperAgent-Subnetz gesendet.
5. Bei Empfang der Übertragung erhält der Agent eine für die Aktualisierung erforderliche Katalogmindestversion.
6. Der Agent durchsucht die verteilten Repositories nach einer Site, die diese Katalogmindestversion enthält.
7. Sobald er ein passendes Repository gefunden hat, führt er den Aktualisierungs-Task aus.

Wenn der Agent die Übertragung nicht empfängt (beispielsweise weil der Client-Computer ausgeschaltet ist oder keine SuperAgents vorhanden sind), wird die Katalogmindestversion bei der nächsten Agent-Server-Kommunikation übertragen. Dadurch wird der Vorgang gestartet.

Wenn der Agent eine Benachrichtigung von einem SuperAgent empfängt, erhält er die Liste der aktualisierten Pakete. Wenn der Agent die neue Katalogversion bei der nächsten Agent-Server-Kommunikation erhält, verfügt er nicht über die Liste der zu aktualisierenden Pakete, und alle verfügbaren Pakete werden aktualisiert.

Voraussetzungen

Folgende Voraussetzungen müssen für das Implementieren der globalen Aktualisierung erfüllt sein:

- Ein SuperAgent muss den gleichen ASSC-Schlüssel (Schlüssel für sichere Agenten-Server-Kommunikation) wie die Agenten verwenden, die seine Reaktivierung empfangen.
- In jedem Übertragungssegment ist ein SuperAgent installiert. Verwaltete Systeme können nur dann eine SuperAgent-Reaktivierung empfangen, wenn sich ein SuperAgent im gleichen Übertragungssegment befindet. Bei der globalen Aktualisierung wird die SuperAgent-Reaktivierung verwendet, um die Agenten über neu verfügbare Aktualisierungen zu benachrichtigen.
- Verteilte Repositories wurden in der Umgebung eingerichtet und konfiguriert. McAfee SuperAgent-Repositories werden empfohlen, sind jedoch nicht erforderlich. Die globale Aktualisierung funktioniert bei allen Typen von verteilten Repositories.
- Wenn Sie SuperAgent-Repositories verwenden, muss auf den verwalteten Systemen der Zugriff auf das Repository mit den Aktualisierungen möglich sein. Damit Systeme Reaktivierungsaufrufe empfangen können, muss in jedem Übertragungssegment zwar ein SuperAgent vorhanden sein, SuperAgent-Repositories sind jedoch nicht erforderlich.

Automatisches Ausbringen von Aktualisierungspaketen per globaler Aktualisierung

Sie können auf dem Server die globale Aktualisierung aktivieren, damit vom Benutzer festgelegte Aktualisierungspakete automatisch auf verwalteten Systemen ausgebracht werden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie **Globale Aktualisierung** aus, und klicken Sie dann unten auf der Seite auf **Bearbeiten**.

2 Wählen Sie auf der Seite **Globale Aktualisierung: Bearbeiten** neben **Status** die Option **Aktiviert** aus.

3 Ändern Sie das **Zufallsintervall** bei Bedarf.

Jede Client-Aktualisierung wird zu einem zufälligen Zeitpunkt innerhalb dieses Zufallsintervalls durchgeführt, wodurch die Netzwerkbelastung besser verteilt wird. Die Standardeinstellung beträgt **20 Minuten**.

Wenn Sie zum Beispiel 1.000 Clients mit dem standardmäßigen Zufallsintervall von 20 Minuten aktualisieren, werden in diesem Zeitraum etwa 50 Clients pro Minute aktualisiert, wodurch das Netzwerk und der Server entlastet werden. Ohne die Zufallsgenerierung würden alle 1.000 Clients gleichzeitig aktualisiert werden.

4 Wählen Sie neben **Pakettypen** aus, welche Pakete eine Aktualisierung auslösen.

Die globale Aktualisierung wird nur dann ausgelöst, wenn für die hier ausgewählten Komponenten neue Pakete in das Master-Repository eingecheckt werden oder in einen anderen Zweig verschoben werden. Wählen Sie die Komponenten daher sorgfältig aus.

- **Signaturen und Scan-Module** – Wählen Sie **Host Intrusion Prevention-Inhalt** aus, wenn erforderlich.

Von der Auswahl eines Pakettyps hängt ab, wodurch eine globale Aktualisierung initialisiert wird (nicht, was dabei aktualisiert wird). Agenten erhalten während der globalen Aktualisierung eine Liste von aktualisierten Paketen. Anhand dieser Liste installieren Agenten nur die Aktualisierungen, die erforderlich sind. So aktualisieren Agenten zum Beispiel nicht alle Pakete, sondern nur die, die seit der letzten Aktualisierung geändert wurden.

5 Klicken Sie abschließend auf **Speichern**.

Nachdem die globale Aktualisierung aktiviert wurde, wird eine Aktualisierung ausgelöst, sobald eines der ausgewählten Pakete eingecheckt oder in einen anderen Zweig verschoben wird.

Achten Sie darauf, dass ein Task vom Typ "Jetzt abrufen" ausgeführt wird und ein regelmäßiger Server-Task vom Typ "Repository-Abruf" geplant ist, wenn die automatische Aktualisierung fertig konfiguriert ist.

15 Manuelle Verwaltung von Paketen und Aktualisierungen

Wenn Sie neue Produkte außerhalb ihrer normalen geplanten Task-Routinen ausbringen möchten, können Sie diese manuell einchecken.

Inhalt

- *Hinzufügen von Produkten zur Verwaltung*
- *Manuelles Einchecken von Paketen*
- *Löschen von DAT- oder Scan-Modul-Paketen aus dem Master-Repository*
- *Manuelles Verschieben von DAT- und Scan-Modul-Paketen zwischen Zweigen*
- *Manuelles Einchecken von Scan-Modul-, DAT- und EXTRA.DAT-Aktualisierungspaketen*

Hinzufügen von Produkten zur Verwaltung

Die Erweiterung für ein Produkt muss installiert werden, damit dieses Produkt von ePolicy Orchestrator verwaltet werden kann.

Bevor Sie beginnen

Vergewissern Sie sich, dass sich die Erweiterungsdatei in einem Speicherort auf dem Netzwerk befindet, auf den zugegriffen werden kann.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie in der ePolicy Orchestrator-Konsole auf **Menü** | **Software** | **Erweiterungen** | **Erweiterung installieren**.

Das Master-Repository darf nicht durch mehrere Tasks gleichzeitig aktualisiert werden. Wenn Sie versuchen, während einer Aktualisierung des Master-Repositorys eine Erweiterung zu installieren, wird die folgende Fehlermeldung angezeigt:

Die Erweiterung kann nicht installiert werden. com.mcafee.core.cdm.CommandException: Das ausgewählte Paket kann während eines Abruf-Tasks nicht eingecheckt werden.

Warten Sie, bis die Aktualisierung des Master-Repositorys abgeschlossen ist, und versuchen Sie dann erneut, die Erweiterung zu installieren.

2 Wechseln Sie zur Erweiterungsdatei, wählen Sie sie aus, und klicken Sie auf **OK**.

3 Überprüfen Sie, ob der Produktname in der Liste **Erweiterungen** angezeigt wird.

Manuelles Einchecken von Paketen

Checken Sie Ausbringungspakete manuell in das **Master-Repository** ein, damit sie von ePolicy Orchestrator ausgebracht werden können.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Starten Sie den Assistenten Paket einchecken.

   a Wählen Sie die folgenden Optionen aus: **Menü** | **Software** | **Master-Repository**.

   b Klicken Sie auf **Paket einchecken**.

2 Wählen Sie den Pakettyp aus, wechseln Sie dann zur gewünschten Paketdatei, und wählen Sie sie aus.

3 Klicken Sie auf **Weiter**.

4 Bestätigen oder konfigurieren Sie Folgendes:

- **Paketinfo** – Bestätigen Sie, dass dies das richtige Paket ist.
- **Zweig**: Wählen Sie den Zweig aus. Wenn in der Umgebung neue Pakete vor dem Ausbringen in der gesamten Produktionsumgebung getestet werden müssen, McAfee sollten Sie beim Einchecken von Paketen den Zweig **Test** verwenden. Nach dem Testen können Sie die Pakete in den Zweig **Aktuell** verschieben, indem Sie auf **Menü** | **Software** | **Master-Repository** klicken.
- **Optionen**: Wählen Sie eine der folgenden Optionen aus:
  - **Vorhandenes Paket in den Zweig "Vorherige" verschieben**: Bei Auswahl dieser Option werden Pakete im Master-Repository aus dem Zweig **Aktuell** in den Zweig **Vorherige** verschoben, wenn ein neueres Paket des gleichen Typs eingecheckt wird. Diese Option ist nur dann verfügbar, wenn Sie unter **Zweig** die Option **Aktuell** auswählen.
- **Paket-Signaturen**: Gibt an, ob das Paket von McAfee oder einem Drittanbieter stammt.

5 Klicken Sie auf **Speichern**, um mit dem Einchecken des Pakets zu beginnen, und warten Sie dann, während das Paket eingecheckt wird.

Das neue Paket wird auf der Registerkarte **Master-Repository** in der Liste **Pakete im Master-Repository** angezeigt.

Löschen von DAT- oder Scan-Modul-Paketen aus dem Master-Repository

Sie können DAT- oder Scan-Modul-Pakete aus dem Master-Repository löschen. Wenn Sie regelmäßig neue Aktualisierungspakete einchecken, ersetzen diese die älteren Versionen oder verschieben sie in den Zweig Vorherige, sofern Sie den Zweig Vorherige verwenden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Software** | **Master-Repository**.

2 Klicken Sie in der Zeile mit dem Paket auf **Löschen**.

3 Klicken Sie auf **OK**.

Manuelles Verschieben von DAT- und Scan-Modul-Paketen zwischen Zweigen

Sie können Pakete nach dem Einchecken in das Master-Repository manuell zwischen den Zweigen Test, Aktuell und Vorherige verschieben.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Software** | **Master-Repository**.

2 Klicken Sie in der Zeile des Pakets auf **Zweig wechseln**.

3 Wählen Sie aus, ob Sie das Paket in einen anderen Zweig verschieben oder kopieren möchten.

4 Wählen Sie aus, welcher Zweig das Paket erhalten soll.

Wenn Sie in Ihrem Netzwerk mit McAfee® NetShield® for NetWare arbeiten, aktivieren Sie **NetShield for NetWare unterstützen**.

5 Klicken Sie auf **OK**.

Manuelles Einchecken von Scan-Modul-, DAT- und EXTRA.DAT-Aktualisierungspaketen

Sie können Aktualisierungspakete manuell in das Master-Repository einchecken, um sie anschließend mithilfe von ePolicy Orchestrator auszubringen. Einige Pakete können nur manuell eingecheckt werden.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Starten Sie den Assistenten Paket einchecken.

a Wählen Sie die folgenden Optionen aus: **Menü** | **Software** | **Master-Repository**.

b Klicken Sie auf **Paket einchecken**.

2 Wählen Sie den Pakettyp aus, wechseln Sie zu einer Paketdatei, wählen Sie sie aus, und klicken Sie dann auf **Weiter**.

3 Wählen Sie einen Zweig aus:

- **Aktuell** – Hiermit werden die Pakete ohne vorherigen Test verwendet.
- **Test**: Hiermit werden die Pakete zuvor in einer Testumgebung getestet.

Nach dem Testen können Sie die Pakete in den Zweig **Aktuell** verschieben, indem Sie auf **Menü** | **Software** | **Master-Repository** klicken.

- **Vorherige** – Hiermit wird das Paket mithilfe der vorherigen Version empfangen.

4 Wählen Sie neben **Optionen** die Option **Vorhandenes Paket in den Zweig "Vorherige" verschieben** aus, um das vorhandene Paket (vom gleichen Typ wie das, das Sie einchecken) in den Zweig **Vorherige** zu verschieben.

5 Klicken Sie auf **Speichern**, um mit dem Einchecken des Pakets zu beginnen. Warten Sie, während das Paket eingecheckt wird.

Das neue Paket wird auf der Seite **Master-Repository** in der Liste **Pakete im Master-Repository** angezeigt.

16 Richtlinienverwaltung

Mithilfe von Richtlinien wird sichergestellt, dass die Funktionen eines Produkts auf verwalteten Systemen korrekt konfiguriert sind.

Das Verwalten von Produkten von einer zentralen Stelle aus ist eine Hauptfunktion von ePolicy Orchestrator. Erreichen können Sie dies, indem Sie Produktrichtlinien anwenden und erzwingen. Mit Richtlinien stellen Sie sicher, dass die Funktionen von Produkten ordnungsgemäß konfiguriert sind. Client-Tasks werden als geplante Aktionen auf den verwalteten Systemen ausgeführt, auf denen sich Client-seitige Software befindet.

Inhalt

- *Richtlinien und Richtlinienerzwingung*
- *Richtlinienanwendung*
- *Erstellen und Verwalten von Richtlinien*
- *Erstmaliges Konfigurieren von Richtlinien*
- *Verwalten von Richtlinien*
- *Aufbewahrung von Richtlinien und Tasks: Bearbeiten, Seite*
- *Richtlinienzuweisungsregeln*
- *Erstellen von Abfragen zur Richtlinienverwaltung*
- *Erstellen einer Abfrage zum Definieren der Compliance*
- *Generieren von Compliance-Ereignissen*
- *Anzeigen der Richtlinieninformationen*
- *Freigeben von Richtlinien zwischen McAfee ePO-Servern*
- *Verteilen einer Richtlinie an mehrere McAfee ePO-Server*
- *Fragen zur Richtlinienverwaltung*
- *Richtlinie zuweisen, Seite*

Richtlinien und Richtlinienerzwingung

Eine *Richtlinie* ist eine Sammlung von Einstellungen, die Sie erstellen, konfigurieren und dann erzwingen. Mit Richtlinien können Sie gewährleisten, dass die verwaltete Sicherheits-Software richtig konfiguriert ist und funktioniert.

Richtlinienkategorien

Die Richtlinieneinstellungen für die meisten Produkte sind nach *Kategorien* zusammengefasst. Jede Richtlinienkategorie bezieht sich auf eine spezielle Teilgruppe von Richtlinieneinstellungen. Richtlinien werden nach Kategorien erstellt. Auf der Seite Richtlinienkatalog werden Richtlinien nach Produkt und Kategorie angezeigt. Wenn Sie eine vorhandene Richtlinie öffnen oder eine neue Richtlinie erstellen, werden die Richtlinieneinstellungen in Registerkarten organisiert.

Wo werden Richtlinien angezeigt?

Klicken Sie zum Anzeigen aller Richtlinien einer bestimmten Richtlinienkategorie auf **Menü** | **Richtlinie** | **Richtlinienkatalog**, und wählen Sie dann in den Dropdown-Listen das Produkt und die Kategorie aus. Auf der Seite Richtlinienkatalog werden nur Richtlinien der Produkte angezeigt, für die Sie über Berechtigungen verfügen.

Wenn Sie wissen möchten, welche Richtlinien pro Produkt auf eine bestimmte Gruppe der Systemstruktur angewendet werden, klicken Sie auf **Menü** | **Abschnitt Systeme** | **Systemstruktur** | **Zugewiesene Richtlinien**, wählen Sie eine Gruppe aus, und wählen Sie dann in der Dropdown-Liste ein Produkt aus.

Für jede Kategorie gibt es eine Richtlinie McAfee Default. Diese Richtlinien können Sie weder löschen, bearbeiten, exportieren noch umbenennen, Sie können sie jedoch duplizieren und die Kopie bearbeiten.

Festlegen der Richtlinienerzwingung

Sie können für jedes verwaltete Produkt oder jede verwaltete Komponente festlegen, ob der Agent sämtliche oder keine der Richtlinienbestimmungen für dieses Produkt oder diese Komponente erzwingt.

Auf der Seite Zugewiesene Richtlinien können Sie auswählen, ob Richtlinien für Produkte oder Komponenten bei der ausgewählten Gruppe erzwungen werden sollen.

Auf der Seite Richtlinienkatalog können Sie Richtlinienzuweisungen anzeigen und sehen, wo sie angewendet werden und ob sie erzwungen werden. Darüber hinaus können Sie die Richtlinienerzwingung sperren, um Änderungen an der Erzwingung unterhalb des gesperrten Knotens zu verhindern.

Wenn die Richtlinienerzwingung deaktiviert ist, erhalten Systeme in der angegebenen Gruppe während der Agent-Server-Kommunikation keine aktualisierten Sitelists. Dies kann dazu führen, dass diese verwalteten Systeme nicht wie erwartet funktionieren. Beispiel: Sie konfigurieren verwaltete Systeme so, dass sie mit dem Agenten-Handler A kommunizieren sollen, die Richtlinienerzwingung ist jedoch deaktiviert. Dann erhalten die verwalteten Systeme die neue Sitelist mit dieser Information nicht und melden sich daher bei einem anderen Agenten-Handler, der in einer abgelaufenen Sitelist aufgeführt ist.

Wann werden Richtlinien erzwungen?

Wenn Sie Richtlinieneinstellungen neu konfigurieren, werden die neuen Einstellungen bei der nächsten Agent-Server-Kommunikation an die verwalteten Systeme übermittelt und dort erzwungen. Die Häufigkeit dieser Kommunikation wird von der Einstellung für das Agent-Server-Kommunikationsintervall (ASKI) auf der Registerkarte Allgemein der McAfee Agent-Richtlinienseiten oder durch den Client-Task-Plan für die McAfee Agent-Reaktivierung bestimmt (je nachdem, wie Sie die Agent-Server-Kommunikation implementieren). Standardmäßig ist dieses Intervall auf einen Wert von 60 Minuten eingestellt.

Sobald die Richtlinieneinstellungen auf dem verwalteten System wirksam sind, wird die Erzwingung der Richtlinieneinstellungen durch den Agenten einem regulären Intervall lokal fortgesetzt. Dieses Erzwingungsintervall wird durch die Einstellung Richtlinienerzwingungsintervall auf der Registerkarte Allgemein der McAfee Agent-Richtlinienseiten bestimmt. Standardmäßig ist dieses Intervall auf fünf Minuten festgelegt.

Richtlinieneinstellungen für McAfee-Produkte werden im Richtlinienerzwingungsintervall sofort und – wenn Richtlinieneinstellungen geändert wurden – bei jeder Agent-Server-Kommunikation erzwungen.

Exportieren und Importieren von Richtlinien

Wenn Sie mehrere Server haben, können Sie Richtlinien zwischen diesen über XML-Dateien exportieren und importieren. Auf diese Weise müssen Sie eine Richtlinie nur einmal erstellen.

Sie können einzelne oder alle Richtlinien für ein bestimmtes Produkt exportieren und importieren.

Sie können diese Funktion auch verwenden, um bei einer Neuinstallation des Servers Sicherungskopien von Richtlinien zu erstellen.

Richtlinienfreigabe

Eine andere Möglichkeit zum Übertragen von Richtlinien zwischen Servern ist die Richtlinienfreigabe. Durch Freigeben von Richtlinien können Sie Richtlinien auf einem Server verwalten und diese dann über die McAfee ePO-Konsole auf vielen anderen Servern verwenden.

Richtlinienanwendung

Richtlinien werden auf jedes System durch *Vererbung* oder *Zuweisung* angewendet.

Vererbung

Die Richtlinienvererbung bestimmt, ob die Richtlinieneinstellungen und Client-Tasks für eine Gruppe oder ein System vom jeweiligen übergeordneten Element übernommen werden. In der Standardeinstellung ist die Vererbung für die gesamte Systemstruktur aktiviert.

Wenn Sie diese Vererbung unterbrechen, indem Sie an einer bestimmten Stelle in der Systemstruktur eine neue Richtlinie zuweisen, wird diese Richtlinie von allen untergeordneten Gruppen und Systemen geerbt, für die festgelegt ist, dass sie die Richtlinie von diesem Zuweisungspunkt erben.

Zuweisung

Sie können eine Richtlinie im Richtlinienkatalog beliebigen Gruppen oder Systemen zuweisen. Über die Zuweisung können Sie Richtlinieneinstellungen für einen bestimmten Zweck einmal definieren und die Richtlinie dann auf mehrere Stellen anwenden.

Wenn Sie einer bestimmten Gruppe der Systemstruktur eine neue Richtlinie zuweisen, wird diese Richtlinie von allen untergeordneten Gruppen und Systemen geerbt, für die festgelegt ist, dass sie die Richtlinie von diesem Zuweisungspunkt erben.

Sperren von Zuweisungen

Sie können die Zuweisung einer Richtlinie für Gruppen oder Systeme sperren. Durch das Sperren von Zuweisungen wird verhindert, dass andere Benutzer folgende Aufgaben ausführen:

- Benutzer mit entsprechenden Berechtigungen auf der gleichen Ebene der Systemstruktur versehentlich eine Richtlinie austauschen.
- Benutzer mit niedrigeren Berechtigungen (oder den gleichen Berechtigungen, aber auf einer niedrigeren Ebene der Systemstruktur) die Richtlinie austauschen.

Die Sperrung von Zuweisungen wird mit den Richtlinieneinstellungen vererbt.

Das Sperren von Zuweisungen ist nützlich, wenn Sie eine bestimmte Richtlinie an der Spitze der Systemstruktur zuweisen und dabei sicherstellen möchten, dass diese Richtlinie nicht an anderer Stelle in der Systemstruktur durch Benutzer ausgetauscht wird.

Das Sperren von Zuweisungen sperrt nur die Zuweisung der Richtlinie, verhindert aber nicht, dass der Besitzer der Richtlinie Änderungen an den Einstellungen vornehmen kann. Wenn Sie eine Richtlinienzuweisung sperren möchten, sollten Sie daher sicherstellen, dass Sie der Besitzer der Richtlinie sind.

Richtlinienbesitz

Alle Richtlinien stehen auf der Seite Richtlinienkatalog zur Verfügung. Damit Benutzer keine Richtlinien anderer Benutzer bearbeiten können, ist jeder Richtlinie ein Besitzer zugewiesen. Dabei handelt es sich um den Benutzer, der sie erstellt hat.

Der Besitz einer Richtlinie gewährleistet, dass eine Richtlinie von niemandem außer dem Benutzer, der sie erstellt hat, geändert oder gelöscht werden kann. Jeder Benutzer kann auf der Seite Richtlinienkatalog Richtlinien zuweisen, aber nur der Benutzer, der sie erstellt hat, kann sie bearbeiten.

Wenn Sie verwalteten Systemen eine Richtlinie zuweisen, deren Besitzer Sie nicht sind, müssen Sie Folgendes beachten: Wird diese benannte Richtlinie durch den Besitzer geändert, werden diese Änderungen auf allen Systemen wirksam, denen diese Richtlinie zugewiesen ist. Daher sollten Sie, wenn Sie eine Richtlinie verwenden möchten, die sich im Besitz eines anderen Benutzers befindet, zunächst ein Duplikat dieser Richtlinie erstellen und dann dieses Duplikat einem Speicherort zuweisen. Auf diese Weise werden Sie Besitzer der zugewiesenen Richtlinie.

Sie können mehrere Benutzer als Besitzer für eine einzige Richtlinie festlegen.

Erstellen und Verwalten von Richtlinien

Sie können auf der Seite **Richtlinienkatalog** Richtlinien erstellen und verwalten.

Aufgaben

- *Erstellen einer Richtlinie auf der Seite Richtlinienkatalog* auf Seite 206
  Mit dem Richtlinienkatalog erstellte benutzerdefinierte Richtlinien sind standardmäßig keinen Gruppen oder Systemen zugewiesen. Sie können Richtlinien vor oder nach dem Ausbringen eines Produkts erstellen.
- *Verwalten einer vorhandenen Richtlinie auf der Seite Richtlinienkatalog* auf Seite 207
  Sie können eine Richtlinie bearbeiten, duplizieren, umbenennen und löschen.

Erstellen einer Richtlinie auf der Seite Richtlinienkatalog

Mit dem Richtlinienkatalog erstellte benutzerdefinierte Richtlinien sind standardmäßig keinen Gruppen oder Systemen zugewiesen. Sie können Richtlinien vor oder nach dem Ausbringen eines Produkts erstellen.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Öffnen Sie das Dialogfeld **Neue Richtlinie**.

   a Klicken Sie auf **Menü** | **Richtlinie** | **Richtlinienkatalog**.

   b Wählen Sie in den Dropdown-Listen das Produkt und die Kategorie aus.

   Alle für die ausgewählte Kategorie erstellten Richtlinien werden im Bereich **Details** angezeigt.

   c Klicken Sie auf **Neue Richtlinie**.

2 Wählen Sie in der Dropdown-Liste **Richtlinie auf Grundlage dieser vorhandenen Richtlinie erstellen** die Richtlinie aus, die Sie duplizieren möchten.

3 Geben Sie einen Namen für die neue Richtlinie ein, und klicken Sie auf **OK**.

   Die Richtlinie wird im Richtlinienkatalog angezeigt.

4 Klicken Sie auf den Namen der neuen Richtlinie.

Der Assistent Richtlinieneinstellungen wird geöffnet.

5 Bearbeiten Sie die Richtlinieneinstellungen nach Bedarf.

6 Klicken Sie auf **Speichern**.

Verwalten einer vorhandenen Richtlinie auf der Seite Richtlinienkatalog

Sie können eine Richtlinie bearbeiten, duplizieren, umbenennen und löschen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie zum Auswählen einer vorhandenen Richtlinie auf **Menü** | **Richtlinie** | **Richtlinienkatalog**, und wählen Sie dann in den Dropdown-Listen das Produkt und die Kategorie aus.

Alle für die ausgewählte Kategorie erstellten Richtlinien werden im Detailbereich angezeigt.

2 Wählen Sie eine der folgenden Aktionen aus.

Aktion	Vorgehensweise
Bearbeiten von Richtlinieneinstellungen Die Anzahl der betroffenen Systeme wird oben auf der Seite angezeigt.	1 Suchen Sie die Richtlinie, und klicken Sie dann auf den Richtliniennamen. 2 Bearbeiten Sie die Einstellungen nach Bedarf, und klicken Sie dann auf **Speichern**.
Duplizieren einer Richtlinie	1 Suchen Sie die Richtlinie, und klicken Sie dann in der Zeile der Richtlinie auf **Duplizieren**. Das Dialogfeld Vorhandene Richtlinie duplizieren wird angezeigt. 2 Geben Sie den Namen für die neue Richtlinie in das Feld ein, und klicken Sie auf **OK**. Die neue Richtlinie wird auf der Seite Richtlinienkatalog angezeigt. 3 Klicken Sie auf die neue Richtlinie in der Liste. 4 Bearbeiten Sie die Einstellungen nach Bedarf, und klicken Sie dann auf **Speichern**. Die neue Richtlinie wird im Detailbereich angezeigt.

Aktion	Vorgehensweise
Umbenennen einer Richtlinie	1 Suchen Sie die Richtlinie, und klicken Sie dann in der Zeile der Richtlinie auf **Umbenennen**. Das Dialogfeld Richtlinie umbenennen wird angezeigt. 2 Geben Sie einen neuen Namen für die vorhandene Richtlinie ein, und klicken Sie dann auf **OK**. Die umbenannte Richtlinie wird im Detailbereich angezeigt.
Löschen einer Richtlinie	1 Suchen Sie die Richtlinie, und klicken Sie dann in der Zeile der Richtlinie auf **Löschen**. 2 Klicken Sie auf **OK**, wenn Sie dazu aufgefordert werden. Die gelöschte Richtlinie wird aus dem Detailbereich entfernt.

Erstmaliges Konfigurieren von Richtlinien

Gehen Sie wie nachfolgend allgemein beschrieben vor, wenn Sie Ihre Richtlinien zum ersten Mal konfigurieren.

1 Planen Sie Produktrichtlinien für die Segmente Ihrer Systemstruktur.

2 Erstellen Sie Richtlinien für Gruppen und Systeme, und weisen Sie sie diesen zu.

Verwalten von Richtlinien

Sie können Richtlinien in Ihrer Umgebung zuweisen und verwalten.

Die Anzahl der betroffenen Systeme wird oben auf der Seite angezeigt.

Aufgaben

- *Ändern der Besitzer einer Richtlinie* auf Seite 209
  Standardmäßig wird der Ersteller einer Richtlinie auch als ihr Besitzer festgelegt. Wenn Sie über die erforderlichen Berechtigungen verfügen, können Sie den Besitzer einer Richtlinie ändern.
- *Verschieben von Richtlinien zwischen McAfee ePO-Servern* auf Seite 210
  Um Richtlinien zwischen McAfee ePO-Servern zu verschieben, müssen Sie die Richtlinie auf der Seite **Richtlinienkatalog** des Quell-Servers in eine XML-Datei exportieren und dann in die Seite **Richtlinienkatalog** auf dem Ziel-Server importieren.
- *Zuweisen einer Richtlinie zu einer Systemstrukturgruppe* auf Seite 211
  Sie können einer bestimmten Gruppe der Systemstruktur eine Richtlinie zuweisen. Diese Richtlinienzuweisung können Sie vor oder nach der Produktausbringung vornehmen.
- *Zuweisen einer Richtlinie zu einem verwalteten System* auf Seite 211
  Sie können einem bestimmten verwalteten System eine Richtlinie zuweisen. Diese Richtlinienzuweisung können Sie vor oder nach der Produktausbringung vornehmen.
- *Zuweisen einer Richtlinie zu Systemen in einer Systemstrukturgruppe* auf Seite 212
  Sie können mehreren verwalteten Systemen innerhalb einer Gruppe eine Richtlinie zuweisen. Diese Richtlinienzuweisung können Sie vor oder nach der Produktausbringung vornehmen.
- *Erzwingen von Richtlinien für ein Produkt in einer Systemstrukturgruppe* auf Seite 212
  Sie können die Richtlinienerzwingung für ein Produkt in einer Gruppe aktivieren oder deaktivieren. Die Richtlinienerzwingung ist standardmäßig aktiviert und wird in der Systemstruktur vererbt.
- *Erzwingen von Richtlinien für ein Produkt auf einem System* auf Seite 213
  Sie können die Richtlinienerzwingung für ein Produkt auf einem verwalteten System aktivieren oder deaktivieren. Die Richtlinienerzwingung ist standardmäßig aktiviert und wird in der Systemstruktur vererbt.
- *Kopieren von Richtlinienzuweisungen* auf Seite 213
  Sie können Richtlinienzuweisungen aus einer Gruppe oder einem System in eine andere Gruppe bzw. ein anderes System kopieren. Das ist eine einfache Methode, um mehrere Zuweisungen zwischen Gruppen und Systemen an unterschiedlichen Stellen der Systemstruktur freizugeben.

Ändern der Besitzer einer Richtlinie

Standardmäßig wird der Ersteller einer Richtlinie auch als ihr Besitzer festgelegt. Wenn Sie über die erforderlichen Berechtigungen verfügen, können Sie den Besitzer einer Richtlinie ändern.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Richtlinie** | **Richtlinienkatalog**, und wählen Sie dann das **Produkt** und die **Kategorie** aus.

Alle für die ausgewählte Kategorie erstellten Richtlinien werden im Detailbereich angezeigt.

2 Suchen Sie die gewünschte Richtlinie, und klicken Sie dann auf den Besitzer der Richtlinie.

Die Seite **Richtlinienbesitz** wird angezeigt.

3 Wählen Sie in der Liste die Besitzer der Richtlinie aus, und klicken Sie anschließend auf **OK**.

Verschieben von Richtlinien zwischen McAfee ePO-Servern

Um Richtlinien zwischen McAfee ePO-Servern zu verschieben, müssen Sie die Richtlinie auf der Seite **Richtlinienkatalog** des Quell-Servers in eine XML-Datei exportieren und dann in die Seite **Richtlinienkatalog** auf dem Ziel-Server importieren.

Aufgaben

- *Exportieren einer einzelnen Richtlinie* auf Seite 210
  Exportieren Sie eine einzelne Richtlinie in eine XML-Datei, und verwenden Sie diese Datei dann, um die Richtlinie in einen anderen McAfee ePO-Server zu importieren oder um die Datei zur Sicherung der Richtlinie aufzubewahren.
- *Exportieren aller Richtlinien eines Produkts* auf Seite 210
- *Importieren von Richtlinien* auf Seite 211
  Sie können eine XML-Richtliniendatei importieren. Der Import verläuft immer gleich, unabhängig davon, ob Sie eine einzelne oder alle benannten Richtlinien exportiert haben.

Exportieren einer einzelnen Richtlinie

Exportieren Sie eine einzelne Richtlinie in eine XML-Datei, und verwenden Sie diese Datei dann, um die Richtlinie in einen anderen McAfee ePO-Server zu importieren oder um die Datei zur Sicherung der Richtlinie aufzubewahren.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Richtlinie** | **Richtlinienkatalog**, und wählen Sie dann in den Dropdown-Listen das **Produkt** und die **Kategorie** aus.

   Alle für die ausgewählte Kategorie erstellten Richtlinien werden im Bereich **Details** angezeigt.

2 Suchen Sie die Richtlinie, und klicken Sie dann neben der Richtlinie auf **Exportieren**.

   Die Seite **Exportieren** wird angezeigt.

3 Klicken Sie mit der rechten Maustaste auf den Link, um die Datei herunterzuladen und zu speichern.

4 Geben Sie einen Namen für die XML-Richtliniendatei ein, und speichern Sie sie.

Wenn Sie diese Datei auf einen anderen McAfee ePO-Server importieren möchten, müssen Sie sicherstellen, dass der McAfee ePO-Zielserver auf diesen Speicherort zugreifen kann.

Exportieren aller Richtlinien eines Produkts

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Richtlinie** | **Richtlinienkatalog**, und wählen Sie dann das **Produkt** und die **Kategorie** aus.

   Alle für die ausgewählte Kategorie erstellten Richtlinien werden im Detailbereich angezeigt.

2 Klicken Sie neben **Produktrichtlinien** auf **Exportieren**. Die Seite **Exportieren** wird angezeigt.

3 Klicken Sie mit der rechten Maustaste auf den Link, um die Datei herunterzuladen und zu speichern.

Wenn Sie diese Datei auf einen anderen McAfee ePO-Server importieren möchten, müssen Sie sicherstellen, dass der McAfee ePO-Zielserver auf diesen Speicherort zugreifen kann.

Importieren von Richtlinien

Sie können eine XML-Richtliniendatei importieren. Der Import verläuft immer gleich, unabhängig davon, ob Sie eine einzelne oder alle benannten Richtlinien exportiert haben.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Richtlinie** | **Richtlinienkatalog**, und klicken Sie dann neben **Produktrichtlinien** auf **Importieren**.

2 Suchen und wählen Sie die XML-Richtliniendatei aus, und klicken Sie dann auf **OK**.

3 Wählen Sie die zu importierenden Richtlinien aus, und klicken Sie auf **OK**.

Die Richtlinien werden zum Richtlinienkatalog hinzugefügt.

Zuweisen einer Richtlinie zu einer Systemstrukturgruppe

Sie können einer bestimmten Gruppe der Systemstruktur eine Richtlinie zuweisen. Diese Richtlinienzuweisung können Sie vor oder nach der Produktausbringung vornehmen.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Zugewiesene Richtlinien**, und wählen Sie dann in der Dropdown-Liste ein Produkt aus.

Jede pro Kategorie zugewiesene Richtlinie wird im Detailbereich angezeigt.

2 Suchen Sie die gewünschte Richtlinienkategorie, und klicken Sie dann auf **Zuweisungen bearbeiten**.

3 Wenn die Richtlinie geerbt wurde, wählen Sie neben **Geerbt von** die Option **Vererbung unterbrechen und ab hier Richtlinie und Einstellungen zuweisen** aus.

4 Wählen Sie in der Dropdown-Liste **Zugewiesene Richtlinie** die Richtlinie aus.

An dieser Stelle können Sie auch die Einstellungen der ausgewählten Richtlinie bearbeiten oder eine Richtlinie erstellen.

5 Legen Sie fest, ob die Richtlinienvererbung gesperrt werden soll.

Durch das Sperren der Richtlinienvererbung wird verhindert, dass Systemen, die diese Richtlinie erben, eine andere Richtlinie zugewiesen wird.

6 Klicken Sie auf **Speichern**.

Zuweisen einer Richtlinie zu einem verwalteten System

Sie können einem bestimmten verwalteten System eine Richtlinie zuweisen. Diese Richtlinienzuweisung können Sie vor oder nach der Produktausbringung vornehmen.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Systeme**, und wählen Sie dann unter Systemstruktur eine Gruppe aus.

Alle Systeme, die sich in dieser Gruppe (aber nicht ihren Untergruppen) befinden, werden im Detailbereich angezeigt.

2 Wählen Sie ein System aus, und klicken Sie auf **Aktionen** | **Agent** | **Richtlinien auf einem einzelnen System ändern**.

Die Seite **Richtlinienzuweisung** für dieses System wird angezeigt.

3 Wählen Sie ein Produkt aus.

Die Kategorien der ausgewählten Produkte werden mit der dem System zugewiesenen Richtlinie aufgeführt.

4 Suchen Sie die gewünschte Richtlinienkategorie, und klicken Sie dann auf **Zuweisungen bearbeiten**.

5 Wenn die Richtlinie geerbt wurde, wählen Sie neben **Vererbt von** die Option **Vererbung unterbrechen und ab hier Richtlinie und Einstellungen zuweisen** aus.

6 Wählen Sie in der Dropdown-Liste **Zugewiesene Richtlinie** die Richtlinie aus.

An dieser Stelle können Sie auch die Einstellungen der ausgewählten Richtlinie bearbeiten oder eine Richtlinie erstellen.

7 Legen Sie fest, ob die Richtlinienvererbung gesperrt werden soll.

Durch das Sperren der Richtlinienvererbung wird verhindert, dass Systemen, die diese Richtlinie erben, eine andere Richtlinie zugewiesen wird.

8 Klicken Sie auf **Speichern**.

Zuweisen einer Richtlinie zu Systemen in einer Systemstrukturgruppe

Sie können mehreren verwalteten Systemen innerhalb einer Gruppe eine Richtlinie zuweisen. Diese Richtlinienzuweisung können Sie vor oder nach der Produktausbringung vornehmen.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Systeme**, und wählen Sie dann in der Systemstruktur eine Gruppe aus.

Alle Systeme, die sich in dieser Gruppe (aber nicht ihren Untergruppen) befinden, werden im Detailbereich angezeigt.

2 Wählen Sie die gewünschten Systeme aus, und klicken Sie dann auf **Aktionen** | **Agent** | **Richtlinie und Vererbung zuweisen**.

Die Seite **Richtlinie zuweisen** wird angezeigt.

3 Wählen Sie das **Produkt**, die **Kategorie** und die **Richtlinie** in den entsprechenden Dropdown-Listen aus.

4 Aktivieren Sie **Vererbung zurücksetzen** oder **Vererbung unterbrechen**, und klicken Sie dann auf **Speichern**.

Erzwingen von Richtlinien für ein Produkt in einer Systemstrukturgruppe

Sie können die Richtlinienerzwingung für ein Produkt in einer Gruppe aktivieren oder deaktivieren. Die Richtlinienerzwingung ist standardmäßig aktiviert und wird in der Systemstruktur vererbt.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Zugewiesene Richtlinien**, und wählen Sie dann in der **Systemstruktur** eine Gruppe aus.
2. Wählen Sie das gewünschte Produkt aus, und klicken Sie dann auf den Link neben **Erzwingungsstatus**.

   Die Seite **Erzwingen für** wird angezeigt.
3. Wenn Sie den Erzwingungsstatus ändern möchten, müssen Sie zuerst **Vererbung unterbrechen und ab hier Richtlinie und Einstellungen zuweisen** auswählen.
4. Wählen Sie neben **Erzwingungsstatus** entsprechend **Wird erzwungen** oder **Wird nicht erzwungen** aus.
5. Legen Sie fest, ob die Richtlinienvererbung gesperrt werden soll.

   Durch das Sperren der Richtlinienvererbung wird verhindert, dass die Vererbung für Gruppen und Systeme unterbrochen wird, die diese Richtlinie erben.
6. Klicken Sie auf **Speichern**.

Erzwingen von Richtlinien für ein Produkt auf einem System

Sie können die Richtlinienerzwingung für ein Produkt auf einem verwalteten System aktivieren oder deaktivieren. Die Richtlinienerzwingung ist standardmäßig aktiviert und wird in der Systemstruktur vererbt.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Systeme**, und wählen Sie dann unter **Systemstruktur** die Gruppe aus, zu der das System gehört.

   Alle Systeme, die zu der ausgewählten Gruppe gehören, werden im Detailbereich angezeigt.
2. Wählen Sie ein System aus, und klicken Sie auf **Aktionen** | **Richtlinien auf einem einzelnen System ändern**.

   Die Seite **Richtlinienzuweisung** wird angezeigt.
3. Wählen Sie ein **Produkt** aus, und klicken Sie dann neben **Erzwingungsstatus** auf **Wird erzwungen**.

   Die Seite Erzwingen für wird angezeigt.
4. Wenn Sie den Erzwingungsstatus ändern möchten, müssen Sie zuerst **Vererbung unterbrechen und ab hier Richtlinie und Einstellungen zuweisen** auswählen.
5. Wählen Sie neben **Erzwingungsstatus** entsprechend **Wird erzwungen** oder **Wird nicht erzwungen** aus.
6. Klicken Sie auf **Speichern**.

Kopieren von Richtlinienzuweisungen

Sie können Richtlinienzuweisungen aus einer Gruppe oder einem System in eine andere Gruppe bzw. ein anderes System kopieren. Das ist eine einfache Methode, um mehrere Zuweisungen zwischen Gruppen und Systemen an unterschiedlichen Stellen der Systemstruktur freizugeben.

Aufgaben

- *Kopieren von Richtlinienzuweisungen aus einer Gruppe* auf Seite 214
  Sie können Richtlinienzuweisungen aus einer Gruppe in der Systemstruktur in eine andere kopieren.
- *Kopieren von Richtlinienzuweisungen aus einem System* auf Seite 214
  Kopieren Sie Richtlinienzuweisungen aus einem bestimmten System.
- *Einfügen von Richtlinienzuweisungen in eine Gruppe* auf Seite 214
  Nachdem Sie die Richtlinienzuweisungen aus einer Gruppe oder einem System kopiert haben, können Sie sie in eine Gruppe einfügen.
- *Einfügen von Richtlinienzuweisungen für ein bestimmtes System* auf Seite 215
  Nachdem Sie die Richtlinienzuweisungen aus einer Gruppe oder einem System kopiert haben, fügen Sie sie in ein bestimmtes System ein.

Kopieren von Richtlinienzuweisungen aus einer Gruppe

Sie können Richtlinienzuweisungen aus einer Gruppe in der Systemstruktur in eine andere kopieren.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Zugewiesene Richtlinien**, und wählen Sie dann in der Systemstruktur eine Gruppe aus.

2 Klicken Sie auf **Aktionen** | **Zuweisungen kopieren**.

3 Wählen Sie die Produkte oder Funktionen aus, für die Sie Richtlinienzuweisungen kopieren möchten, und klicken Sie dann auf **OK**.

Kopieren von Richtlinienzuweisungen aus einem System

Kopieren Sie Richtlinienzuweisungen aus einem bestimmten System.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Systeme**, und wählen Sie dann in der Systemstruktur eine Gruppe aus.

Die Systeme, die zu der ausgewählten Gruppe gehören, werden im Detailbereich angezeigt.

2 Wählen Sie ein System aus, und klicken Sie auf **Aktionen** | **Agent** | **Richtlinien auf einem einzelnen System ändern**.

3 Klicken Sie auf **Aktionen** | **Richtlinienzuweisungen kopieren**, wählen Sie die Produkte oder Funktionen aus, für die Sie Richtlinienzuweisungen kopieren möchten, und klicken Sie dann auf **OK**.

Einfügen von Richtlinienzuweisungen in eine Gruppe

Nachdem Sie die Richtlinienzuweisungen aus einer Gruppe oder einem System kopiert haben, können Sie sie in eine Gruppe einfügen.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Zugewiesene Richtlinien**, und wählen Sie dann in der **Systemstruktur** die gewünschte Gruppe aus.

2 Klicken Sie im Detailbereich auf **Aktionen**, und wählen Sie **Zuweisungen einfügen** aus.

Wenn der Gruppe bereits für einige Kategorien Richtlinien zugewiesen sind, wird die Seite **Richtlinienzuweisungen außer Kraft setzen** angezeigt.

Beim Einfügen von Richtlinienzuweisungen wird die Richtlinie **Richtlinien und Tasks erzwingen** in der Liste angezeigt. Diese Richtlinie steuert den Erzwingungsstatus anderer Richtlinien.

3 Wählen Sie aus, welche Richtlinienkategorien Sie durch die kopierten Richtlinien ersetzen möchten, und klicken Sie dann auf **OK**.

Einfügen von Richtlinienzuweisungen für ein bestimmtes System

Nachdem Sie die Richtlinienzuweisungen aus einer Gruppe oder einem System kopiert haben, fügen Sie sie in ein bestimmtes System ein.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Systeme**, und wählen Sie dann in der Systemstruktur eine Gruppe aus.

Alle Systeme, die zu der ausgewählten Gruppe gehören, werden im Detailbereich angezeigt.

2 Wählen Sie das System aus, zu dem Sie Richtlinienzuweisungen einfügen möchten, und klicken Sie dann auf **Aktionen** | **Agent** | **Richtlinien auf einem einzelnen System ändern**.

3 Klicken Sie im Detailbereich auf **Aktionen** | **Zuweisungen einfügen**.

Wenn dem System bereits für einige Kategorien Richtlinien zugewiesen sind, wird die Seite **Richtlinienzuweisungen außer Kraft setzen** angezeigt.

Beim Einfügen von Richtlinienzuweisungen wird die Richtlinie **Richtlinien und Tasks erzwingen** in der Liste angezeigt. Diese Richtlinie steuert den Erzwingungsstatus anderer Richtlinien.

4 Bestätigen Sie das Ersetzen von Zuweisungen.

Aufbewahrung von Richtlinien und Tasks: Bearbeiten, Seite

Auf dieser Seite können Sie festlegen, ob Daten zu Richtlinien und Client-Tasks entfernt werden, wenn Sie eine Verwaltungserweiterung für ein Produkt löschen.

Tabelle 16-1 Optionsbeschreibungen

Option	Beschreibung
Aufbewahrung von Richtlinien und Tasks	Gibt an, ob Daten von Richtlinien und Client-Tasks entfernt werden, wenn Sie eine Verwaltungserweiterung für ein Produkt löschen. Folgende Optionen stehen zur Auswahl: • **Richtlinien- und Client-Task-Daten beibehalten** • **Richtlinien- und Client-Task-Daten entfernen**: Mit der Standardeinstellung werden Daten von Richtlinien und Client-Tasks entfernt.

Richtlinienzuweisungsregeln

Durch Richtlinienzuweisungsregeln sinkt der Aufwand für das Verwalten einer Vielzahl von Richtlinien für einzelne Benutzer oder Systeme, die bestimmten Kriterien entsprechen, während für die gesamte Systemstruktur allgemeinere Richtlinien geführt werden.

Durch diese abgestufte Richtlinienzuweisung werden die Instanzen mit unterbrochener Vererbung in der Systemstruktur begrenzt, um den Richtlinieneinstellungen gerecht zu werden, die für bestimmte Benutzer oder Systeme benötigt werden. Richtlinienzuweisungen können auf benutzerspezifischen oder systemspezifischen Kriterien basieren:

- *Benutzerbasierte Richtlinien* – Das sind Richtlinien, die mindestens ein benutzerspezifisches Kriterium enthalten. So können Sie zum Beispiel eine Richtlinienzuweisungsregel erstellen, die für alle Benutzer in der Entwicklungsabteilungsgruppe erzwungen wird. Anschließend können Sie eine andere Richtlinienzuweisungsregel für Mitglieder Ihrer IT-Abteilung erstellen, sodass sich diese bei jedem Computer im Netzwerk der Entwicklungsabteilung mit den Zugriffsrechten anmelden können, die sie zur Behebung von Problemen auf einem bestimmten System in diesem Netzwerk benötigen. Benutzerbasierte Richtlinien *können* auch systembasierte Kriterien enthalten.
- *Systembasierte Richtlinien* – Das sind Richtlinien, die nur systembasierte Kriterien enthalten. So können Sie zum Beispiel eine Richtlinienzuweisungsregel erstellen, die bei allen Servern im Netzwerk, die mit bestimmten Tags gekennzeichnet sind, oder auf allen Systemen, die sich in einem bestimmten Speicherort in der Systemstruktur befinden, umgesetzt wird. Systembasierte Richtlinien können *keine* benutzerbasierten Kriterien enthalten.

Priorität von Richtlinienzuweisungsregeln

Richtlinienzuweisungsregeln können priorisiert werden, um die Wartung der Richtlinienzuweisungsverwaltung zu vereinfachen. Wenn Sie für eine Regel eine Priorität festlegen, wird sie vor anderen Zuweisungen mit einer niedrigeren Priorität erzwungen.

In einigen Fällen kann dies dazu führen, dass Regeleinstellungen außer Kraft gesetzt werden. Beispiel: Ein System ist in zwei Richtlinienzuweisungsregeln (Regel A und B) enthalten. Die Regel A hat die Prioritätsstufe 1 und räumt den zugehörigen Systemen einen unbegrenzten Zugriff auf Internetinhalte ein. Die Regel B hat die Prioritätsstufe 2 und schränkt den Zugriff desselben Systems auf Internetinhalte stark ein. In diesem Szenario wird die Regel A erzwungen, da sie eine höhere Priorität hat. Daher erhält das System uneingeschränkten Zugriff auf Internetinhalte.

Zusammenarbeit von Richtlinien für mehrere Richtlinienplätze mit der Priorität von Richtlinienzuweisungsregeln

Die Priorität von Regeln wird bei Richtlinien für mehrere Richtlinienplätze nicht berücksichtigt. Wenn eine einzelne Regel angewendet wird, die Richtlinien für mehrere Richtlinienplätze derselben Produktkategorie enthält, werden alle Einstellungen der Richtlinien für mehrere Richtlinienplätze kombiniert. Ebenso werden beim Anwenden mehrerer Regeln, die Einstellungen für Richtlinien für mehrere Richtlinienplätze enthalten, alle Einstellungen aus den einzelnen Richtlinien für mehrere Richtlinienplätze kombiniert. Dadurch besteht die angewendete Richtlinie aus einer Kombination der Einstellungen aller einzelnen Regeln.

Wenn Richtlinien für mehrere Richtlinienplätze aggregiert werden, erfolgt dies nur mit Richtlinien für mehrere Richtlinienplätze des gleichen Typs. Richtlinien für mehrere Richtlinienplätze, die mithilfe von Richtlinienzuweisungsregeln zugewiesen sind, werden jedoch nicht mit Richtlinien für mehrere Richtlinienplätze aggregiert, die in der Systemstruktur zugewiesen sind. In der Systemstruktur zugewiesene Richtlinien für mehrere Richtlinienplätze werden von Richtlinien für mehrere Richtlinienplätze außer Kraft gesetzt, die mithilfe von Richtlinienzuweisungsregeln zugewiesen sind. Außerdem haben benutzerbasierte Richtlinien Vorrang vor systembasierten Richtlinien.

Szenario: Steuerung des Internetzugriffs mithilfe von Richtlinien für mehrere Richtlinienplätze

In Ihrer Systemstruktur befindet sich eine Gruppe mit dem Namen "Technik", die aus Systemen besteht, die mit "IsServer" oder "IsLaptop" gekennzeichnet sind. Richtlinie A ist in der Systemstruktur allen Systemen in dieser Gruppe zugewiesen. Wenn Richtlinie B mithilfe einer Richtlinienzuweisungsregel an einer beliebigen Stelle oberhalb der Gruppe Technik in der Systemstruktur zugewiesen wird, setzt sie die Einstellungen der Richtlinie A außer Kraft und erlaubt den Zugriff auf das Internet durch Systeme, die mit "IsLaptop" gekennzeichnet sind. Wenn Richtlinie C einer beliebigen Gruppe zugewiesen wird, die sich in der Systemstruktur oberhalb der Gruppe Technik befindet, wird dadurch Benutzern aus der Benutzergruppe Admin der Internetzugriff auf allen Systemen erlaubt, d. h. auch auf denjenigen, die sich in der Gruppe Technik" befinden und mit "IsServer" gekennzeichnet sind.

Richtlinientyp	Zuweisungstyp	Richtlinienname	Richtlinieneinstellungen
Allgemeine Richtlinie	In der Systemstruktur zugewiesene Richtlinie	A	Unterbindet den Internetzugriff auf allen Systemen, denen die Richtlinien zugewiesen ist.
Systembasiert	Richtlinienzuweisungsregel	B	Erlaubt den Internetzugriff auf Systemen, die mit dem Tag "IsLaptop" gekennzeichnet sind.
Systembasiert	Richtlinienzuweisungsregel	C	Erlaubt allen Benutzern aus der Benutzergruppe "admin" auf allen Systemen den uneingeschränkten Internetzugriff.
Benutzerbasiert	Richtlinienzuweisungsregel	C	Erlaubt allen Benutzern aus der Benutzergruppe "admin" auf allen Systemen den uneingeschränkten Internetzugriff.

Ausschließen von Active Directory-Objekten aus aggregierten Richtlinien

Da Regeln, die aus Richtlinien für mehrere Richtlinienplätze bestehen, ohne Beachtung von Prioritäten auf zugewiesene Systeme angewendet werden, muss die Aggregation von Richtlinieneinstellungen an einigen Stellen möglicherweise verhindert werden. Die Aggregation von Einstellungen aus benutzerbasierten Richtlinien für mehrere Richtlinienplätze über mehrere Richtlinienzuweisungsregeln hinweg lässt sich verhindern, indem Sie einen Benutzer (oder andere Active Directory-Objekte wie eine Gruppe oder Organisationseinheit) beim Erstellen der Richtlinienzuweisungsregel ausschließen. Weitere Informationen zur Verwendung von Richtlinien für mehrere Richtlinienplätze in Richtlinienzuweisungsregeln finden Sie in der Produktdokumentation des von Ihnen verwendeten verwalteten Produkts.

Benutzerbasierte Richtlinienzuweisungen

Mit benutzerbasierten Richtlinienzuweisungsregeln können Sie benutzerspezifische Richtlinienzuweisungen erstellen.

Diese Zuweisungen werden auf dem Zielsystem erzwungen, wenn sich ein Benutzer anmeldet.

Bei der ersten Anmeldung eines Benutzers bei einem verwalteten System kann es zu einer geringfügigen Verzögerung kommen, während von McAfee Agent eine Verbindung mit dem zugewiesenen Server hergestellt wird, um die für diesen Benutzer spezifischen Richtlinienzuweisungen abzurufen. Während dieses Zeitraums kann der Benutzer nur auf die Funktionen zugreifen, die gemäß der Standardrichtlinie auf dem Computer (in der Regel die sicherste Richtlinie) zulässig sind.

Auf einem verwalteten System werden die Benutzer, die sich beim Netzwerk anmelden, vom Agenten erfasst. Die für die einzelnen Benutzer erstellten Richtlinienzuweisungen werden mithilfe von Push auf das System übertragen, bei dem sich diese Benutzer anmelden, und während jeder Agent-Server-Kommunikation zwischengespeichert. Auf dem McAfee ePO-Server werden die Richtlinien angewendet, die Sie jedem Benutzer zugewiesen haben.

Wenn Sie benutzerbasierte Richtlinienzuweisungen verwenden möchten, müssen Sie einen LDAP-Server registrieren und für den Gebrauch bei Ihrem McAfee ePO-Server konfigurieren.

Informationen zu systembasierten Richtlinienzuweisungen

Mithilfe systembasierter Richtlinien können Systemen Richtlinien nach systembasierten Kriterien zugewiesen werden.

Eine systembasierte Richtlinie kann mithilfe zweier Typen von systembasierten Kriterien zugewiesen werden:

- **Speicherort in der Systemstruktur** – Bei allen Richtlinienzuweisungsregeln muss ein Speicherort in der Systemstruktur angegeben werden.
- **Tags** – Richtlinien müssen Systemen anhand der angewendeten Tags zugewiesen werden.

Sobald Sie ein Tag definiert und auf Systeme angewendet haben, können Sie eine Richtlinienzuweisungsregel erstellen, nach der Richtlinien auf jedes System angewendet werden sollen, das mit diesem Tag gekennzeichnet ist. Diese Funktion ist besonders nützlich, wenn alle Systeme eines bestimmten Typs über die gleiche Sicherheitsrichtlinie verfügen sollen, unabhängig von ihrer Position in der Systemstruktur.

Zuweisen von systembasierten Richtlinien mithilfe von Tags

Sie können Tags nutzen, um die automatische Richtlinienzuweisung zu vereinfachen.

Systembasierte Richtlinien werden anhand von Auswahlkriterien zugewiesen, die Sie mit dem Generator für Richtlinienzuweisungen definieren. Sie können jedem System, das mit einem Tag versehen werden kann, anhand dieses Tags eine bestimmte Richtlinie zuweisen.

Szenario: Erstellen neuer SuperAgents mithilfe von Tags

Sie möchten einen neuen Satz von SuperAgents in der Umgebung erstellen, haben jedoch nicht die Zeit, manuell die Systeme in der Systemstruktur zu bestimmen, auf denen sich diese SuperAgents befinden sollen. Stattdessen können Sie den Tag-Generator verwenden, um alle den gewünschten Kriterien entsprechenden Systeme mit einem neuen Tag zu kennzeichnen: "istSuperAgent". Nachdem Sie das Tags erstellt haben, können Sie eine Richtlinienzuweisungsregel erstellen, mit der die SuperAgent-Richtlinieneinstellungen auf alle Systeme mit dem Tag "istSuperAgent" angewendet werden.

Sobald Sie das Tag erstellt haben, können Sie die Aktion **Tag-Kriterien ausführen** auf der Seite Tag-Katalog verwenden, damit jedem mit dem neuen Tag versehenen System, wenn es sich in regelmäßigen Abständen meldet, die neue Richtlinie gemäß der Richtlinienzuweisungsregel istSuperAgent zugewiesen wird.

Erstellen von Richtlinienzuweisungsregeln

Durch die Erstellung von Richtlinienzuweisungsregeln können Sie Richtlinien für Benutzer oder Systeme anhand konfigurierter Regelkriterien erzwingen.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Öffnen Sie den **Generator für Richtlinienzuweisungen**.

   a Klicken Sie auf **Menü** | **Richtlinie** | **Richtlinienzuweisungsregeln**.

   b Klicken Sie auf **Neue Zuweisungsregel**.

2 Geben Sie die Details für diese Richtlinienzuweisungsregel an. Dazu gehören die folgenden:

   - Ein eindeutiger **Name** und eine **Beschreibung**.
   - Der **Regeltyp**. Vom angegebenen Regeltyp hängt es ab, welche Kriterien auf der Seite **Auswahlkriterien** verfügbar sind.

   Die Priorität für neue Richtlinienzuweisungsregeln wird standardmäßig sequenziell basierend auf der Anzahl der vorhandenen Regeln zugewiesen. Nachdem Sie die Regel erstellt haben, können Sie die Priorität bearbeiten, indem Sie auf der Seite **Richtlinienzuweisungsregeln** auf **Priorität bearbeiten** klicken.

3 Klicken Sie auf **Weiter**.

4 Klicken Sie auf **Richtlinie hinzufügen**, um die Richtlinien auszuwählen, die von dieser Richtlinienzuweisungsregel erzwungen werden sollen.

5 Klicken Sie auf **Weiter**.

6 Geben Sie die Kriterien an, die in dieser Regel verwendet werden sollen. Ihre Kriterienauswahl bestimmt, welchen Systemen oder Benutzern diese Richtlinie zugewiesen wird.

7 Überprüfen Sie die Zusammenfassung, und klicken Sie dann auf **Speichern**.

Verwalten von Richtlinienzuweisungsregeln

Führen Sie bei der Arbeit mit Richtlinienzuweisungsregeln allgemeine Verwaltungs-Tasks durch.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Richtlinie** | **Richtlinienzuweisungsregeln**.

2 Wählen Sie eine der folgenden Aktionen aus:

Aktionen	Vorgehensweise
Löschen von Richtlinienzuweisungsregeln	Klicken Sie in der Zeile mit der ausgewählten Zuweisung auf **Löschen**.
Bearbeiten von Richtlinienzuweisungsregeln	Klicken Sie auf die ausgewählte Zuweisung. Der Assistent Generator für Richtlinienzuweisungen wird angezeigt. Führen Sie die Schritte auf den einzelnen Seiten des Assistenten durch, um diese Richtlinienzuweisungsregel zu ändern.
Exportieren von Richtlinienzuweisungsregeln	Wählen Sie **Aktionen**	**Exportieren** aus. Die Seite Exportieren wird geöffnet, auf der Sie die Datei PolicyAssignmentRules.xml anzeigen oder herunterladen können.
Importieren von Richtlinienzuweisungsregeln	Wählen Sie **Aktionen**	**Importieren** aus. Das Dialogfeld Richtlinienzuweisungsregeln importieren wird geöffnet, in dem Sie die zuvor heruntergeladene Datei `PolicyAssignmentRules.xml` suchen können. Sie werden aufgefordert, die in der Datei enthaltenen Regeln auszuwählen, die importiert werden sollen. Sie können auswählen, welche Regeln importiert werden sollen. Falls Regeln in der Datei einen identischen Namen haben wie Regeln, die sich bereits in der Liste **Richtlinienzuweisungsregeln** befinden, können Sie darüber hinaus auswählen, welche Regeln beibehalten werden sollen.
Bearbeiten der Priorität einer Richtlinienzuweisungsregel	Klicken Sie auf **Aktionen**	**Priorität bearbeiten**. Die Seite Priorität bearbeiten wird geöffnet, auf der Sie die Priorität von Richtlinienzuweisungsregeln mittels Ziehen und Ablegen ändern.
Anzeigen der Zusammenfassung einer Richtlinienzuweisungsregel	Klicken Sie in der Zeile mit der ausgewählten Zuweisung auf **>**.

Erstellen von Abfragen zur Richtlinienverwaltung

Sie können die einem verwalteten System zugewiesenen oder die in der Systemhierarchie unterbrochenen Richtlinien abrufen.

Sie können eine der folgenden Abfragen zur Richtlinienverwaltung erstellen:

- **Angewendete Richtlinien** – Diese Abfrage ruft Richtlinien ab, die einem angegebenen verwalteten System zugewiesen sind.
- **Vererbung unterbrochen** – Diese Abfrage ruft Informationen zu Richtlinien ab, die in der Systemhierarchie unterbrochen sind.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie **Menü** | **Berichterstellung** | **Abfragen und Berichte**aus, und klicken Sie dann auf **Neue Abfrage**.

Der Abfrage-Generator wird geöffnet.

2 Wählen Sie auf der Seite Ergebnistyp in der Liste **Funktionsgruppe** den Eintrag **Richtlinienverwaltung** aus.

3 Wählen Sie einen Ergebnistyp aus, und klicken Sie dann auf **Weiter**, um die Seite Diagramm anzuzeigen:

- **Angewandte Client-Tasks**
- **Angewendete Richtlinien**
- **Unterbrochene Vererbung für Client-Task-Zuweisung**
- **Unterbrochene Vererbung für Richtlinienzuweisung**

4 Wählen Sie den Diagramm- oder Tabellentyp zum Anzeigen der primären Ergebnisse der Abfrage aus, und klicken Sie dann auf **Weiter**.

Die Seite Spalten wird angezeigt.

Wenn Sie **Boolesches Kreisdiagramm** auswählen, müssen Sie die Kriterien konfigurieren, die in der Abfrage enthalten sein sollen.

5 Wählen Sie die Spalten aus, die in der Abfrage enthalten sein sollen, und klicken Sie dann auf **Weiter**.

Die Seite Filter wird angezeigt.

6 Wählen Sie Eigenschaften aus, um die Suchergebnisse einzugrenzen, und klicken Sie dann auf **Ausführen**.

Auf der Seite Nicht gespeicherte Abfrage werden die Ergebnisse der Abfrage angezeigt, für die auch Aktionen durchgeführt werden können.

Ausgewählte Eigenschaften werden im Inhaltsbereich mit Operatoren angezeigt. Mit diesen können Sie Kriterien festlegen, nach denen die für die jeweilige Eigenschaft zurückgegebenen Daten eingegrenzt werden.

7 Auf der Seite Nicht gespeicherte Abfrage können Sie alle verfügbaren Aktionen für Elemente in sämtlichen Tabellen oder Drilldown-Tabellen durchführen.

- Wenn für die Abfrage nicht die erwarteten Ergebnisse zurückgegeben wurden, klicken Sie auf **Abfrage bearbeiten**, um zum Abfrage-Generator zurückzukehren und die Details der Abfrage zu bearbeiten.
- Wenn Sie die Abfrage nicht speichern möchten, klicken Sie auf **Schließen**.
- Wenn Sie diese Abfrage zu einem späteren Zeitpunkt erneut verwenden möchten, klicken Sie auf **Speichern**, und fahren Sie dann mit dem nächsten Schritt fort.

8 Geben Sie auf der Seite Abfrage speichern einen Namen für die Abfrage ein, fügen Sie Anmerkungen hinzu, und wählen Sie dann eine der folgenden Optionen aus:

- **Neue Gruppe** – Geben Sie den Namen der neuen Gruppe ein, und wählen Sie eine der folgenden Optionen:
  - **Private Gruppe (Eigene Gruppen)**
  - **Öffentliche Gruppe (Freigegebene Gruppen)**
- **Vorhandene Gruppe** – Wählen Sie die Gruppe in der Liste Freigegebene Gruppen aus.

9 Klicken Sie auf **Speichern**.

Erstellen einer Abfrage zum Definieren der Compliance

Compliance-Abfragen sind auf McAfee ePO-Servern erforderlich, deren Daten in Abfragen mit zusammengefassten Daten verwendet werden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie **Menü** | **Berichterstellung** | **Abfragen und Berichte**aus, und klicken Sie dann auf **Neue Abfrage**.
2. Wählen Sie auf der Seite **Ergebnistyp** unter **Funktionsgruppe** den Eintrag Systemverwaltung und unter **Ergebnistypen** die Option Verwaltete Systeme aus, und klicken Sie dann auf **Weiter**.
3. Wählen Sie in der Liste Ergebnisse anzeigen als die Option **Boolesches Kreisdiagramm** aus, und klicken Sie anschließend auf **Kriterien konfigurieren**.
4. Wählen Sie die in die Abfrage einzuschließenden Eigenschaften aus, und legen Sie dann die Operatoren und Werte für jede Eigenschaft fest. Klicken Sie auf **OK**. Wenn die Seite **Diagramm** angezeigt wird, klicken Sie auf **Weiter**.

   Mit diesen Eigenschaften definieren Sie die Compliance für Systeme, die von diesem McAfee ePO-Server verwaltet werden.

5. Wählen Sie die Spalten aus, die in der Abfrage enthalten sein sollen, und klicken Sie dann auf **Weiter**.
6. Wählen Sie die Filter für die Abfrage aus, klicken Sie auf **Ausführen** und anschließend auf **Speichern**.

Generieren von Compliance-Ereignissen

Compliance-Ereignisse werden in Abfragen mit zusammengefassten Daten verwendet, um Daten in einem Bericht zu aggregieren.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Automatisierung** | **Server-Tasks**, und klicken Sie dann auf **Aktionen** | **Neuer Task**.
2. Geben Sie auf der Seite **Beschreibung** einen Namen für den neuen Task ein, und klicken Sie anschließend auf **Weiter**.
3. Wählen Sie im Dropdown-Menü **Aktionen** den Eintrag **Abfrage ausführen** aus.
4. Klicken Sie neben dem Feld **Abfrage** auf die Schaltfläche zum Durchsuchen […], und wählen Sie eine Abfrage aus. Das Dialogfeld **Wählen Sie eine Abfrage in der Liste aus** wird angezeigt, und die Registerkarte **Private Gruppen** ist aktiv.
5. Wählen Sie die Abfrage aus, durch die die Compliance definiert wird. Es sollte sich dabei um eine Standardabfrage handeln, z. B. **Compliance-Übersicht von McAfee Agent** auf der Registerkarte **McAfee-Gruppen**, oder um eine vom Benutzer erstellte Abfrage, z. B. wie unter *Erstellen einer Abfrage zum Definieren der Compliance* beschrieben.
6. Wählen Sie im Dropdown-Menü **Untergeordnete Aktionen** die Option **Compliance-Ereignis generieren** aus, geben Sie den Prozentsatz oder die Anzahl der Zielsysteme an, und klicken Sie dann auf **Weiter**.

   Ereignisse können mit dem Task "Compliance-Ereignis generieren" generiert werden, wenn die Non-Compliance einen festgelegten Prozentsatz oder eine festgelegte Anzahl von Systemen übersteigt.

7 Planen Sie den Task für das erforderliche Zeitintervall zum Erstellen des Berichts **Compliance-Verlauf** ein. Wenn die Compliance zum Beispiel wöchentlich erfasst werden muss, planen Sie den Task zur wöchentlichen Ausführung. Klicken Sie auf **Weiter**.

8 Prüfen Sie die Angaben, und klicken Sie auf **Speichern**.

Anzeigen der Richtlinieninformationen

Sie können detaillierte Informationen zu Richtlinien anzeigen, darunter Informationen über die Besitzer, die Zuweisungen und die Vererbung.

Aufgaben

- *Anzeigen der Gruppen und Systeme, denen eine Richtlinie zugewiesen ist* auf Seite 223
  Sie können Gruppen und Systeme anzeigen, denen eine Richtlinie zugewiesen ist. In dieser Liste werden nur die Zuweisungspunkte angezeigt, aber nicht die einzelnen Knoten oder Systeme, die diese Richtlinie erben.
- *Anzeigen von Richtlinieneinstellungen* auf Seite 224
  Sie können Details zu einer Richtlinie anzeigen, die einer Produktkategorie oder einem System zugewiesen ist.
- *Anzeigen des Richtlinienbesitzes* auf Seite 224
  Sie können die Besitzer einer Richtlinie anzeigen.
- *Anzeigen von Zuweisungen, bei denen die Richtlinienerzwingung deaktiviert ist* auf Seite 224
  Sie können Zuweisungen anzeigen, bei denen die Richtlinienerzwingung (pro Richtlinienkategorie) deaktiviert ist.
- *Anzeigen der einer Gruppe zugewiesenen Richtlinien* auf Seite 225
  Sie können die einer Systemstrukturgruppe zugewiesenen Richtlinien nach Produkt sortiert anzeigen.
- *Anzeigen der einem bestimmten System zugewiesenen Richtlinien* auf Seite 225
  Sie können die Richtlinien anzeigen, die einem bestimmten System in der Systemstrukturgruppe zugewiesen worden.
- *Anzeigen der Richtlinienvererbung für eine Gruppe* auf Seite 225
  Sie können die Richtlinienvererbung einer bestimmten Gruppe anzeigen.
- *Anzeigen und Zurücksetzen einer unterbrochenen Vererbung* auf Seite 226
  Sie können die Gruppen und Systeme ermitteln, bei denen die Richtlinienvererbung unterbrochen wurde.
- *Vergleichen von Richtlinien* auf Seite 226
  Mithilfe der Option Richtlinienvergleich können Sie Richtlinien vergleichen. Auf diese Weise können Sie ermitteln, welche Einstellungen sich unterscheiden und welche identisch sind.

Anzeigen der Gruppen und Systeme, denen eine Richtlinie zugewiesen ist

Sie können Gruppen und Systeme anzeigen, denen eine Richtlinie zugewiesen ist. In dieser Liste werden nur die Zuweisungspunkte angezeigt, aber nicht die einzelnen Knoten oder Systeme, die diese Richtlinie erben.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Richtlinie** | **Richtlinienkatalog**, und wählen Sie dann das Produkt und die Kategorie aus.

Alle für die ausgewählte Kategorie erstellten Richtlinien werden im Detailbereich angezeigt.

2 Klicken Sie unter **Zuweisungen** in der Zeile der Richtlinie auf den Link, der die Anzahl der Gruppen oder Systeme angibt, denen die Richtlinie zugewiesen ist (z. B. **6 Zuweisungen**).

Auf der Seite **Zuweisungen** werden alle Gruppe oder Systeme, denen die Richtlinie zugewiesen ist, mit ihrem Knotennamen und Knotentyp angezeigt.

Anzeigen von Richtlinieneinstellungen

Sie können Details zu einer Richtlinie anzeigen, die einer Produktkategorie oder einem System zugewiesen ist.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Richtlinie** | **Richtlinienkatalog**, und wählen Sie dann das Produkt und die Kategorie aus.

Alle für die ausgewählte Kategorie erstellten Richtlinien werden im Detailbereich angezeigt.

2 Klicken Sie neben eine Richtlinie.

Die Richtlinienseiten werden mit den Einstellungen der Richtlinie angezeigt.

Sie können diese Informationen auch anzeigen, wenn Sie auf die einer bestimmten Gruppe zugewiesenen Richtlinien zugreifen. Klicken Sie zum Zugriff auf diese Informationen auf **Menü** | **Systeme** | **Systemstruktur** | **Zugewiesene Richtlinien** und anschließend in der Spalte **Richtlinie** auf den Link für die ausgewählte Richtlinie.

Anzeigen des Richtlinienbesitzes

Sie können die Besitzer einer Richtlinie anzeigen.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Richtlinie** | **Richtlinienkatalog**, und wählen Sie dann das Produkt und die Kategorie aus.

Alle für die ausgewählte Kategorie erstellten Richtlinien werden im Detailbereich angezeigt.

2 Die Besitzer der Richtlinie werden unter **Besitzer** angezeigt.

Anzeigen von Zuweisungen, bei denen die Richtlinienerzwingung deaktiviert ist

Sie können Zuweisungen anzeigen, bei denen die Richtlinienerzwingung (pro Richtlinienkategorie) deaktiviert ist.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Richtlinie** | **Richtlinienkatalog**, und wählen Sie dann das Produkt und die Kategorie aus.

Alle für die ausgewählte Kategorie erstellten Richtlinien werden im Detailbereich angezeigt.

2 Klicken Sie auf den Link neben **Erzwingungsstatus für Produkt**, der die Anzahl der Zuweisungen anzeigt, bei denen die Erzwingung deaktiviert ist (sofern vorhanden).

   Die Seite **Erzwingen für <Richtlinienname>** wird angezeigt.

3 Klicken Sie auf ein beliebiges Element in der Liste, um zu dessen Seite **Zugewiesene Richtlinien** zu wechseln.

Anzeigen der einer Gruppe zugewiesenen Richtlinien

Sie können die einer Systemstrukturgruppe zugewiesenen Richtlinien nach Produkt sortiert anzeigen.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Zugewiesene Richtlinien**, und wählen Sie dann in der Systemstruktur eine Gruppe aus.

   Im Detailbereich werden alle zugewiesenen Richtlinien nach Produkt geordnet angezeigt.

2 Klicken Sie auf eine beliebige Richtlinie, um deren Einstellungen anzuzeigen.

Anzeigen der einem bestimmten System zugewiesenen Richtlinien

Sie können die Richtlinien anzeigen, die einem bestimmten System in der Systemstrukturgruppe zugewiesen worden.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Systeme**, und wählen Sie dann in der Systemstruktur eine Gruppe aus.

   Alle Systeme, die zu der Gruppe gehören, werden im Detailbereich angezeigt.

2 Wählen Sie das System aus, und klicken Sie auf **Aktionen** | **Agent** | **Richtlinien auf einem einzelnen System ändern**.

3 Wählen Sie das Produkt aus.

   Die diesem System für das Produkt zugewiesenen Richtlinien werden angezeigt.

4 Klicken Sie auf eine beliebige Richtlinie, um deren Einstellungen anzuzeigen.

Anzeigen der Richtlinienvererbung für eine Gruppe

Sie können die Richtlinienvererbung einer bestimmten Gruppe anzeigen.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Zugewiesene Richtlinien**.

   Im Detailbereich werden alle zugewiesenen Richtlinien nach Produkt geordnet angezeigt.

2 In der Richtlinienzeile ist unter **Erben von** der Name der Gruppe aufgeführt, von der die Richtlinie vererbt wurde.

Anzeigen und Zurücksetzen einer unterbrochenen Vererbung

Sie können die Gruppen und Systeme ermitteln, bei denen die Richtlinienvererbung unterbrochen wurde.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Zugewiesene Richtlinien**.

Im Detailbereich werden alle zugewiesenen Richtlinien nach Produkt geordnet angezeigt. In der Zeile mit der Richtlinie ist unter **Vererbung unterbrochen** die Anzahl der Gruppen und Systeme aufgeführt, bei denen die Vererbung dieser Richtlinie unterbrochen ist.

Dies ist die Anzahl der Gruppen bzw. Systeme, bei denen die Richtlinienvererbung unterbrochen ist, nicht die Anzahl der Systeme, die die Richtlinie nicht erben. Wenn beispielsweise nur eine Gruppe die Richtlinie nicht erbt, wird dies durch **1 erbt nicht** angezeigt, unabhängig von der Anzahl der Systeme innerhalb der Gruppe.

2 Klicken Sie auf den Link, der die Anzahl der untergeordneten Gruppen oder Systeme anzeigt, bei denen die Vererbung unterbrochen ist.

Die Seite **Unterbrochene Vererbung: Anzeigen** wird mit einer Liste der Namen dieser Gruppen und Systeme angezeigt.

3 Aktivieren Sie zum Zurücksetzen der Vererbung einer dieser Gruppen oder eines dieser Systeme das Kontrollkästchen neben dem Namen, klicken Sie dann auf **Aktionen**, und wählen Sie **Vererbung zurücksetzen** aus.

Vergleichen von Richtlinien

Mithilfe der Option Richtlinienvergleich können Sie Richtlinien vergleichen. Auf diese Weise können Sie ermitteln, welche Einstellungen sich unterscheiden und welche identisch sind.

Viele der auf der Seite Richtlinienvergleich enthaltenen Werte und Variablen sind produktspezifisch. Informationen zu Optionen, die nicht in der Tabelle aufgeführt sind, finden Sie in der Produktdokumentation des jeweiligen Produkts, von dem die zu vergleichende Richtlinie stammt.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Richtlinienvergleich**, und wählen Sie dann in den Listen die gewünschten Einstellungen für Produkt, Kategorie und **Anzeigen** aus.

Mit diesen Einstellungen werden die zu vergleichenden Richtlinien in den Listen **Richtlinie 1** und **Richtlinie 2** aufgefüllt.

2 Wählen Sie die zu vergleichenden Richtlinien in der Zeile **Richtlinien vergleichen** in den Spalten der Listen **Richtlinie 1** und **Richtlinie 2** aus.

In den beiden obersten Zeilen der Tabelle wird angezeigt, wie viele Einstellungen unterschiedlich und wie viele identisch sind. Wenn Sie weniger Daten anzeigen möchten, können Sie auch die Einstellung **Anzeigen** von **Alle Richtlinieneinstellungen** in **Unterschiede zwischen Richtlinien** oder **Übereinstimmungen zwischen Richtlinien** ändern.

3 Klicken Sie auf **Drucken**, um eine druckfähige Ansicht des Vergleichs anzuzeigen.

Freigeben von Richtlinien zwischen McAfee ePO-Servern

Durch Freigeben von Richtlinien können Administratoren Richtlinien bestimmen, die auf einem Server entwickelt wurden und auf den anderen Servern implementiert werden sollen.

Dazu müssen Administratoren nur drei Schritte durchführen.

1 Bestimmen der freizugebenden Richtlinie

2 Registrieren der Server, die die Richtlinie gemeinsam verwenden sollen

3 Planen eines Server-Tasks zum Verteilen der freigegebenen Richtlinie

Verteilen einer Richtlinie an mehrere McAfee ePO-Server

Sie können die Richtlinienfreigabe zur Verwendung mit mehreren McAfee ePO-Servern konfigurieren. Es wird empfohlen, diese Aufgaben in der hier aufgeführten Reihenfolge auszuführen.

Wenn die Richtlinie nach der Freigabe geändert werden muss, bearbeiten Sie die Richtlinie, und führen Sie den Task zur Richtlinienfreigabe erneut aus. Sie sollten die lokalen Administratoren über die Änderung informieren.

Aufgaben

- *Registrieren von Servern zur Richtlinienfreigabe* auf Seite 227
  Registrieren Sie Server, sodass sie Richtlinien freigeben.
- *Bestimmen von Richtlinien zur Freigabe* auf Seite 227
  Sie können festlegen, dass eine Richtlinie für mehrere McAfee ePO-Server freigegeben werden soll.
- *Planen von Server-Tasks zum Freigeben von Richtlinien* auf Seite 228
  Sie können einen Server-Task planen, damit Richtlinien für mehrere McAfee ePO-Server freigegeben werden.

Registrieren von Servern zur Richtlinienfreigabe

Registrieren Sie Server, sodass sie Richtlinien freigeben.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Konfiguration** | **Registrierte Server**, und klicken Sie dann auf **Neuer Server**. Der Assistent **Generator für registrierte Server** wird mit der Seite **Beschreibung** geöffnet.

2 Wählen Sie im Menü **Server-Typ** den Eintrag **ePO** aus, geben Sie einen Namen und eventuelle Anmerkungen ein, und klicken Sie dann auf **Weiter**. Die Seite **Details** wird angezeigt.

3 Geben Sie die Details zu Ihrem Server an, klicken Sie für **Richtlinienfreigabe** auf **Aktivieren**, und klicken Sie dann auf **Speichern**.

Bestimmen von Richtlinien zur Freigabe

Sie können festlegen, dass eine Richtlinie für mehrere McAfee ePO-Server freigegeben werden soll.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Richtlinie** | **Richtlinienkatalog**, klicken Sie dann auf das Dropdown-Menü **Produkt**, und wählen Sie das Produkt aus, dessen Richtlinie Sie freigeben möchten.

2 Klicken Sie in der Spalte **Aktionen** für die freizugebende Richtlinie auf **Freigeben**.

Freigegebene Richtlinien werden automatisch zu McAfee ePO-Servern gepusht, bei denen die Richtlinienfreigabe aktiviert ist. Wenn Sie in Schritt 2 auf **Freigeben** klicken, wird die Richtlinie unverzüglich zu allen registrierten McAfee ePO-Servern gepusht, bei denen die Richtlinienfreigabe aktiviert ist. Auf ähnliche Weise werden auch Änderungen an freigegebenen Richtlinien gepusht.

Planen von Server-Tasks zum Freigeben von Richtlinien

Sie können einen Server-Task planen, damit Richtlinien für mehrere McAfee ePO-Server freigegeben werden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Öffnen Sie den **Generator für Server-Tasks**.

   a Wählen Sie die folgenden Optionen aus: **Menü** | **Automatisierung** | **Server-Tasks**.

   b Klicken Sie auf **Neuer Task**.

2 Geben Sie auf der Seite Beschreibung den Namen des Tasks und eventuelle Anmerkungen ein, und klicken Sie dann auf **Weiter**.

   Neue Server-Tasks sind standardmäßig aktiviert. Wenn dieser Task nicht aktiviert sein soll, wählen Sie im Feld Planungsstatus die Option **Deaktiviert** aus.

3 Wählen Sie im Dropdown-Menü Aktionen den Eintrag **Richtlinien freigeben** aus, und klicken Sie dann auf **Weiter**.

4 Geben Sie den Zeitplan für den Task an, und klicken Sie dann auf **Weiter**.

5 Überprüfen Sie die zusammengefassten Informationen, und klicken Sie dann auf **Speichern**.

Fragen zur Richtlinienverwaltung

Was ist eine Richtlinie?

Eine Richtlinie ist eine benutzerdefinierte Teilmenge von Produkteinstellungen, die einer Richtlinienkategorie entsprechen. Sie können so viele benannte Richtlinien erstellen, ändern oder löschen, wie es für jede Richtlinienkategorie erforderlich ist.

Was sind die McAfee Default- und die My Default-Richtlinien?

Bei der Installation enthält jede Richtlinienkategorie mindestens zwei Richtlinien. Diese haben die Namen "McAfee Default" und "My Default". Bei Erstinstallationen sind dies die einzigen Richtlinien, die vorhanden sind. Die Konfigurationen sind für beide anfangs identisch.

Die benannten McAfee Default-Richtlinien können weder bearbeitet noch umbenannt oder gelöscht werden. Die Richtlinien vom Typ "My Default" können bearbeitet, umbenannt und gelöscht werden.

Was geschieht mit den untergeordneten Gruppen und Systemen einer Gruppe, der eine neue Richtlinie zugewiesen wird?

Alle untergeordneten Gruppen und Systeme, für die festgelegt ist, dass sie die jeweilige Richtlinienkategorie erben, erben die Richtlinie, die auf eine übergeordnete Gruppe angewendet wird.

Wie wirkt sich die Änderung an einer Richtlinie im Richtlinienkatalog auf die Gruppen und Systeme aus, auf die diese Richtlinie angewendet wird?

Alle Gruppen und Systeme, auf die eine Richtlinie angewendet wird, empfangen an der Richtlinie vorgenommene Änderungen bei der nächsten Agent-zu-Server-Kommunikation. Die Richtlinie wird dann bei jedem Richtlinienerzwingungsintervall erzwungen.

Ich habe eine neue Richtlinie zugewiesen, sie wird aber auf den verwalteten Systemen nicht erzwungen. Warum?

Neue Richtlinienzuweisungen werden erst bei der nächsten Agent-zu-Server-Kommunikation erzwungen.

Ich habe Richtlinienzuweisungen aus einem Quellspeicherort (Gruppe oder System) kopiert und in einem Zielspeicherort eingefügt, aber die im Zielspeicherort zugewiesenen Richtlinien sind mit denen im Quellspeicherort nicht identisch. Warum nicht?

Beim Kopieren und Einfügen von Richtlinienzuweisungen werden nur echte Zuweisungen eingefügt. Wenn der Quellspeicherort eine Richtlinie geerbt hat, die Sie zum Kopieren ausgewählt haben, wurde im Zielspeicherort nur das Vererbungsmerkmal eingefügt. Daher erbt das Ziel dann die Richtlinie (für die jeweilige Richtlinienkategorie) von dem eigenen übergeordneten Element, sodass es sich um eine andere Richtlinie als die handeln kann, die an den Quellspeicherort vererbt wurde.

Richtlinie zuweisen, Seite

Auf dieser Seite können Sie eine McAfee ePO-Konfigurationsrichtlinie zu einer Gruppe oder einem System in der Systemstruktur hinzufügen.

Tabelle 16-2 Optionsdefinitionen

Option	Definition
Richtlinie	Geben Sie die Richtlinie an, die der ausgewählten Gruppe bzw. den ausgewählten Systemen für das entsprechende Produkt und die entsprechende Kategorie zugewiesen wird. Für die Auswahl der Richtlinie stehen drei Listenfelder zur Verfügung: • **Produkt** – Geben Sie das Produkt an, das über Richtlinien verfügt, die verwaltet werden können. • **Kategorie** – Geben Sie die Kategorie an, aus der eine Konfigurationsrichtlinie ausgewählt werden soll. Welche Kategorien verfügbar sind, hängt davon ab, welches Produkt bzw. welche Komponente ausgewählt ist. • **Richtlinie** – Die bestimmte Richtlinie, die Sie zuweisen möchten.
Vererbung	Gibt an, ob Richtlinien, die auf der Ebene Eigenes Unternehmen der Systemstruktur festgelegt wurden, an darunter liegende Gruppen vererbt werden. Untergruppen oder einzelne Systeme erben die Richtlinien ihrer Gruppen.

Siehe auch

Richtlinien und Richtlinienerzwingung auf Seite 203
Richtlinienanwendung auf Seite 205
Erstellen und Verwalten von Richtlinien auf Seite 206
Erstmaliges Konfigurieren von Richtlinien auf Seite 208
Zuweisen einer Richtlinie zu einer Systemstrukturgruppe auf Seite 211
Zuweisen einer Richtlinie zu einem verwalteten System auf Seite 211
Zuweisen einer Richtlinie zu Systemen in einer Systemstrukturgruppe auf Seite 212

17 Client-Tasks

Sie können Client-Tasks erstellen und planen, um die Verwaltung der Systeme in Ihrem Netzwerk zu automatisieren.

Client-Tasks werden für gewöhnlich für folgende Zwecke verwendet:

- Produktausbringung
- Produktfunktionalität
- Upgrades und Aktualisierungen

Weitere Informationen dazu, welche Client-Tasks verfügbar sind und bei welchen Arbeiten diese Tasks Sie unterstützen, finden Sie in der Produktdokumentation Ihrer verwalteten Produkte.

Inhalt

- *Funktionsweise des Client-Task-Katalogs*
- *Ausbringungs-Tasks*
- *Ausbringen von Produkten auf verwaltete Systeme mithilfe des Produktausbringungs-Tasks*
- *Aktualisierungs-Tasks*
- *Verwalten von Client-Tasks*

Funktionsweise des Client-Task-Katalogs

Im Client-Task-Katalog können Sie Client-Task-Objekte erstellen, die Sie auch zur Verwaltung der Systeme in einem Netzwerk verwenden können.

Der Client-Task-Katalog wendet das Konzept logischer Objekte auf ePolicy Orchestrator-Client-Tasks an. Sie können Client-Task-Objekte für vielfältige Verwendungszwecke erstellen, ohne sie sofort zuweisen zu müssen. Daher können Sie diese Objekte beim Zuweisen und Planen von Client-Tasks als wiederverwendbare Komponenten betrachten.

Client-Tasks können auf jeder beliebigen Ebene in der Systemstruktur zugewiesen werden und werden von den Gruppen und Systemen geerbt, die sich auf einer niedrigeren Ebene befinden. Wie bei Richtlinien und Richtlinienzuweisungen können Sie die Vererbung für einen zugewiesenen Client-Task unterbrechen.

Client-Task-Objekte können für mehrere registrierte McAfee ePO-Server in einer Umgebung freigegeben werden. Wenn Client-Task-Objekte als freigegeben festgelegt werden, erhält jeder registrierte Server nach Ausführung des Server-Tasks **Client-Task freigeben** eine Kopie. Alle am Task vorgenommenen Änderungen werden bei jedem Ausführen des Tasks aktualisiert. Wenn ein Client-Task-Objekt freigegeben ist, kann nur dessen Besitzer seine Einstellungen ändern.

Administratoren auf dem Ziel-Server, auf dem ein freigegebener Task empfangen wird, sind keine Besitzer dieses freigegebenen Tasks. Auch keiner der Benutzer auf dem Ziel-Server ist Besitzer von dort eingehenden freigegebenen Task-Objekten.

Ausbringungs-Tasks

Ausbringungs-Tasks sind Client-Tasks, mit denen verwaltete Sicherheitsprodukte aus dem Master-Repository auf verwalteten Systemen ausgebracht werden.

Sie können einzelne Ausbringungs-Task-Objekte mithilfe des Client-Task-Katalogs erstellen sowie verwalten und sie dann Gruppen oder bestimmten Systemen zur Ausführung zuweisen. Alternativ dazu können Sie auch Produktausbringungsprojekte erstellen, um Produkte auf Systemen auszubringen. Mit Produktausbringungsprojekten automatisieren Sie die Erstellung und Planung einzelner Client-Task-Objekte. Darüber hinaus verfügen sie über zusätzliche automatisierte Verwaltungsfunktionen.

Wichtige Aspekte

Berücksichtigen Sie bei der Entscheidung über die Phasen der Produktbereitstellung folgende Punkte:

- Paketgröße und verfügbare Bandbreite zwischen dem Master-Repository und den verwalteten Systemen.Zusätzlich zu einer eventuellen Überlastung des McAfee ePO-Servers oder des Netzwerks kann bei einer Bereitstellung auf zu vielen Systemen die Problembehebung komplizierter werden.
- Möglicherweise ist es sinnvoll, die Produkte nacheinander auf Systemgruppen zu installieren. Wenn die Netzwerkverbindungen schnell sind, versuchen Sie, die Ausbringung jeweils auf mehreren hundert Clients gleichzeitig durchzuführen. Bei langsameren oder weniger zuverlässigen Netzwerkverbindungen sollten Sie es mit kleineren Gruppen versuchen. Während der Ausbringung in der jeweiligen Gruppe sollten Sie die Ausbringung überwachen, Berichte zum Bestätigen erfolgreicher Installationen ausführen und Probleme mit einzelnen Systemen beheben.

Ausbringen von Produkten auf ausgewählten Systemen

Wenn Sie McAfee-Produkte oder -Komponenten ausbringen, die auf einem Teil der verwalteten Systeme installiert sind, gehen Sie wie folgt vor:

1. Verwenden Sie ein Tag, um diese Systeme zu identifizieren.
2. Verschieben Sie die gekennzeichneten Systeme in eine Gruppe.
3. Konfigurieren Sie einen Client-Task für die Produktausbringung in der Gruppe.

Ausbringungspakete für Produkte und Aktualisierungen

Die McAfee ePO-Infrastruktur für die Software-Bereitstellung unterstützt sowohl die Bereitstellung als auch das Aktualisieren von Produkten und Komponenten.

Jedes Produkt, das mit McAfee ePO bereitgestellt werden kann, verfügt über eine Bereitstellungspaketdatei im ZIP-Format. Die ZIP-Datei enthält Installationsdateien für das Produkt, die in einem sicheren Format komprimiert sind. Diese Pakete können mit McAfee ePO auf jedem Ihrer verwalteten Systeme bereitgestellt werden.

Diese ZIP-Dateien werden sowohl für Virusdefinitionsdateien (DAT-Dateien) als auch für Scan-Modul-Aktualisierungspakete verwendet.

Die Produktrichtlinieneinstellungen können vor und nach der Bereitstellung konfiguriert werden. Sie sollten die Richtlinieneinstellungen jedoch vor dem Bereitstellen des Produkts in Ihren Netzwerksystemen konfigurieren. Damit sparen Sie Zeit und stellen sicher, dass Ihre Systeme zum frühestmöglichen Zeitpunkt geschützt werden.

Folgende Pakettypen können mithilfe von Abruf-Tasks oder manuell in das Master-Repository eingecheckt werden.

Unterstützte Pakettypen

Pakettyp	Beschreibung	Ursprung
SuperDAT-Dateien (SDAT.EXE) Dateityp: SDAT.EXE	Die SuperDAT-Dateien enthalten sowohl DAT- als auch Moduldateien in einem Aktualisierungspaket. Bei Problemen mit der Bandbreite sollten Sie DAT- und Moduldateien getrennt aktualisieren.	McAfee-Website. Laden Sie die SuperDAT-Dateien herunter, und checken Sie sie manuell in das Master-Repository ein.
Ergänzende Virusdefinitionsdateien (EXTRA.DAT) Dateityp: Extra.DAT	Die Extra.DAT-Dateien beziehen sich auf eine oder mehrere bestimmte Bedrohungen, die erst nach der zuletzt veröffentlichten DAT-Datei aufgetreten sind. Wenn die Bedrohung einen hohen Schweregrad hat, sollten Sie die Extra.DAT-Datei sofort verteilen und nicht warten, bis die Signatur zur nächsten DAT-Datei hinzugefügt wird. Extra.DAT-Dateien werden auf der McAfee-Website veröffentlicht. Sie können sie über McAfee ePO verteilen. Extra.DAT-Dateien werden nicht mit Abruf-Tasks abgerufen.	McAfee-Website. Laden Sie die zusätzlichen DAT-Dateien herunter, und checken Sie sie manuell in das Master-Repository ein.
Produktausbringungs- und Aktualisierungspakete Dateityp: ZIP	Ein Produktbereitstellungspaket enthält Installations-Software.	Produkt-CD oder heruntergeladene ZIP-Datei. Checken Sie Produktbereitstellungspakete manuell in das Master-Repository ein. In der Dokumentation für das jeweilige Produkt finden Sie die genauen Speicherorte.
McAfee Agent-Sprachpakete Dateityp: ZIP	Ein McAfee Agent-Sprachpaket enthält die Dateien, die für das Bereitstellen der McAfee Agent-Informationen in einer bestimmten Sprache erforderlich sind.	Master-Repository: Während der Installation eingecheckt. Bei zukünftigen McAfee Agent-Versionen müssen die McAfee Agent-Sprachpakete manuell in das Master-Repository eingecheckt werden.

Paket-Signaturen und Sicherheit

Alle von McAfee erstellten und verteilten Pakete werden mit einem Schlüsselpaar signiert, wobei das DSA-Signaturprüfungssystem (Digital Signature Algorithm) und die 168-Bit-3DES-Verschlüsselung zum Einsatz kommen. Schlüssel werden verwendet, um vertrauliche Daten zu ver- oder entschlüsseln.

Sie werden benachrichtigt, wenn Sie Pakete einchecken, die nicht von McAfee signiert sind. Wenn Sie den Paketinhalt als gültig und vertrauenswürdig erachten, können Sie jedoch auch nicht signierte Pakete einchecken. Diese Pakete werden wie oben beschrieben gesichert, aber von McAfee ePO signiert, wenn sie eingecheckt werden.

Für McAfee Agent sind nur die Paketdateien vertrauenswürdig, die von McAfee ePO oder McAfee signiert wurden. Dadurch wird verhindert, dass in Ihrem Netzwerk Pakete empfangen werden, die nicht signiert sind oder aus nicht vertrauenswürdigen Quellen stammen.

Paketreihenfolge und Abhängigkeiten

Wenn eine Produktaktualisierung von einer anderen abhängig ist, müssen Sie die Aktualisierungspakete in der erforderlichen Reihenfolge in das Master-Repository einchecken. Wenn beispielsweise für Patch 2 Patch 1 erforderlich ist, müssen Sie Patch 1 vor Patch 2 einchecken. Die

Reihenfolge der Pakete kann nach dem Einchecken nicht mehr geändert werden. Sie müssen sie entfernen und in der richtigen Reihenfolge erneut einchecken. Wenn Sie ein Paket einchecken, mit dem ein vorhandenes Paket ersetzt wird, wird das vorhandene Paket automatisch entfernt.

Ausbringen von Produkten und Aktualisierungen

Durch die Repository-Infrastruktur von McAfee ePO können Sie Produkt- und Aktualisierungspakete von einer zentralen Stelle aus auf verwalteten Systeme ausbringen. Obwohl das gleiche Repository verwendet wird, gibt es Unterschiede.

Produktausbringungs- und Aktualisierungspakete

Produktausbringungspakete	Aktualisierungspakete
Müssen manuell im Master-Repository eingecheckt werden.	Aktualisierungspakete für DAT-Dateien und Scan-Module können mit einem Abruf-Task automatisch aus der Quellsite kopiert werden. Alle anderen Aktualisierungspakete müssen Sie manuell in das Master-Repository einchecken.
Können im Master-Repository repliziert und mit einem Ausbringungs-Task automatisch auf verwalteten Systemen installiert werden.	Können im Master-Repository repliziert und während einer globalen Aktualisierung automatisch auf verwalteten Systemen installiert werden.
Sofern keine globale Aktualisierung für eine Produktausbringung implementiert wird, muss ein Ausbringungs-Task so konfiguriert und geplant werden, dass das Paket von den verwalteten Systemen abgerufen wird.	Sofern keine globale Aktualisierung für eine Produktaktualisierung implementiert wird, muss ein Client-Aktualisierungs-Task konfiguriert und geplant werden, damit das Paket von den verwalteten Systemen abgerufen wird.

Ausbringen und Aktualisieren von Produkten

Gehen Sie zum Verteilen von Aktualisierungspaketen für DAT-Dateien und Scan-Module wie folgt vor.

1 Checken Sie das Aktualisierungspaket mithilfe eines Abruf-Tasks oder manuell in das Master-Repository ein.

2 Führen Sie eine der folgenden Aktionen aus:

- Wenn Sie die globale Aktualisierung verwenden, erstellen und planen Sie einen Aktualisierungs-Task für Laptop-Systeme, die das Netzwerk verlassen.
- Wenn Sie die globale Aktualisierung nicht verwenden, führen Sie die folgenden Aufgaben aus.
  1 Kopieren Sie mit einem Replizierungs-Task den Inhalt des Master-Repositorys.
  2 Erstellen und planen Sie einen Aktualisierungs-Task für Agenten, um die Aktualisierung auf verwalteten Systemen abzurufen und zu installieren.

Erstmaliges Konfigurieren der Ausbringungen von Produkten und Aktualisierungen

Gehen Sie wie nachfolgend beschrieben vor, um sicherzustellen, dass Ihre Ausbringungen von Produkten und Aktualisierungen fehlerfrei durchgeführt werden.

Wenn Sie zum ersten Mal Produkte ausbringen, gehen Sie wie folgt vor:

1 Konfigurieren Sie Server-Tasks für den Repository-Abruf und die Repository-Replizierung.

2 Checken Sie Produkt- und Aktualisierungspakete mit dem **Software-Manager** in das Master-Repository ein.

3 Konfigurieren Sie Client-Tasks für Produktausbringung und -aktualisierung.

Bereitstellungs-Tags

Wenn ein Bereitstellungs-Task erstellt wird, wird automatisch ein Tag mit dem Task-Namen erstellt und auf die Systeme angewendet, auf denen der Task erzwungen wird.

Diese Tags werden auf der Seite **Tag-Katalog** immer dann zur Gruppe **Bereitstellungs-Tags** hinzugefügt, wenn ein Bereitstellungs-Task erstellt wird und auf den Systemen erzwungen wird. Bei dieser Gruppe handelt es sich um eine schreibgeschützte Gruppe. Tags in dieser Gruppe können nicht manuell angewendet, geändert oder gelöscht werden. Sie können auch nicht in einer Kriterienkonfiguration verwendet werden, um Systeme zu filtern.

Ausbringen von Produkten auf verwaltete Systeme mithilfe des Produktausbringungs-Tasks

Sie können Produkte mithilfe des Client-Tasks **Produktausbringung** auf verwaltete Systeme ausbringen.

Diesen Task können Sie für ein einzelnes System oder für Gruppen in der Systemstruktur erstellen.

Aufgaben

- *Konfigurieren eines Ausbringungs-Tasks für Gruppen verwalteter Systeme* auf Seite 235
  Sie können einen Produktausbringungs-Task so konfigurieren, dass Produkte auf Gruppen verwalteter Systeme in der Systemstruktur ausgebracht werden.
- *Konfigurieren eines Ausbringungs-Tasks zum Installieren von Produkten auf einem verwalteten System* auf Seite 237
  Mithilfe eines Produktausbringungs-Tasks können Sie Produkte auf einem einzelnen System ausbringen.

Konfigurieren eines Ausbringungs-Tasks für Gruppen verwalteter Systeme

Sie können einen Produktausbringungs-Task so konfigurieren, dass Produkte auf Gruppen verwalteter Systeme in der Systemstruktur ausgebracht werden.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Öffnen Sie das Dialogfeld Neuer Task.

   a Wählen Sie die folgenden Optionen aus: **Menü** | **Richtlinie** | **Client-Task-Katalog**.

   b Wählen Sie unter Client-Task-Typen ein Produkt aus.

   c Klicken Sie auf **Neuer Task**.

2 Wählen Sie **Produktbereitstellung** aus, und klicken Sie dann auf **OK**.

3 Geben Sie einen Namen für den Task ein, den Sie erstellen möchten, und fügen Sie gegebenenfalls Anmerkungen hinzu.

4 Wählen Sie neben Zielplattformen die Typen der Plattform für die Ausbringung aus.

5 Wählen Sie neben Produkte und Komponenten Folgendes aus:

- Wählen Sie in der ersten Dropdown-Liste ein Produkt aus. Hier werden die Produkte aufgeführt, die Sie im Master-Repository eingecheckt haben. Wenn das bereitzustellende Produkt hier nicht aufgeführt ist, müssen Sie das Produktpaket einchecken.
- Legen Sie als **Aktion** den Wert **Installieren** fest, und wählen Sie dann die **Sprache** des Pakets und den **Zweig** aus.
- Geben Sie im Textfeld **Befehlszeile** die Befehlszeilenoptionen für die Installation ein. Informationen zu Befehlszeilenoptionen des zu installierenden Produkts finden Sie in der Produktdokumentation.

Sie können auf **+** oder **-** klicken, um Produkte und Komponenten zur angezeigten Liste hinzuzufügen bzw. aus der Liste zu entfernen.

6 Wenn die Sicherheitsprodukte automatisch aktualisiert werden sollen, wählen Sie **Automatische Aktualisierung** aus.

Damit werden auch die HotFixes und Patches für das Produkt automatisch bereitgestellt.

Wenn Sie die automatische Aktualisierung eines Sicherheitsprodukts festlegen, können Sie nicht die **Aktion** auf **Entfernen** festlegen.

7 (Nur Windows) Wählen Sie neben Optionen aus, ob der Task bei jedem Richtlinienvorgang ausgeführt werden soll, und klicken Sie dann auf **Speichern**.

8 Klicken Sie auf **Menü** | **Abschnitt Systeme** | **Systemstruktur** | **Zugewiesene Client-Tasks**, und wählen Sie dann in der Systemstruktur die gewünschte Gruppe aus.

9 Wählen Sie bei **Voreingestellt** den Filter **Produktbereitstellung (McAfee Agent)** aus.

Die einzelnen pro ausgewählter Kategorie zugewiesenen Client-Tasks werden im Bereich Details angezeigt.

10 Klicken Sie auf **Aktionen** | **Neue Client-Task-Zuweisung**.

11 Wählen Sie auf der Seite Task auswählen unter **Produkt** den Eintrag **McAfee Agent** und unter **Task-Typ** den Eintrag **Produktbereitstellung** aus. Wählen Sie anschließend den Task aus, den Sie für die Bereitstellung des Produkts erstellt haben.

12 Wählen Sie neben Tags die Plattformen aus, auf denen Sie die Pakete bereitstellen möchten, und klicken Sie dann auf **Weiter**:

- **Diesen Task an alle Computer senden**
- **Diesen Task nur an Computer senden, die die folgenden Kriterien erfüllen** – Klicken Sie neben dem zu konfigurierenden Kriterium auf **Bearbeiten**, wählen Sie die Tag-Gruppe sowie das für das Kriterium zu verwendende Tag aus, und klicken Sie anschließend auf **OK**.

Um die Liste auf bestimmte Tags zu beschränken, geben Sie den Tag-Namen in das Textfeld unter **Tags** ein.

13 Wählen Sie auf der Seite Plan aus, ob die Planung aktiviert ist, geben Sie die Details für den Zeitplan an, und klicken Sie dann auf **Weiter**.

14 Überprüfen Sie die Zusammenfassung, und klicken Sie dann auf **Speichern**.

Bei jeder geplanten Ausführung wird durch den Bereitstellungs-Task das jeweils aktuelle Sensorpaket auf den Systemen installiert, die den angegebenen Kriterien entsprechen.

Konfigurieren eines Ausbringungs-Tasks zum Installieren von Produkten auf einem verwalteten System

Mithilfe eines Produktausbringungs-Tasks können Sie Produkte auf einem einzelnen System ausbringen.

Erstellen Sie einen Client-Task für die Produktausbringung auf einem einzelnen System, wenn für dieses System Folgendes erforderlich ist:

- Ein installiertes Produkt, das von den anderen Systemen in derselben Gruppe nicht benötigt wird
- Eine andere Planung als bei den anderen Systemen in der Gruppe, wenn sich ein System beispielsweise in einer anderen Zeitzone als die anderen gleichrangigen Systeme befindet

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Öffnen Sie das Dialogfeld Neuer Task.

   a Wählen Sie die folgenden Optionen aus: **Menü** | **Richtlinie** | **Client-Task-Katalog**.

   b Wählen Sie unter Client-Task-Typen ein Produkt aus.

   c Klicken Sie auf **Neuer Task**.

2 Vergewissern Sie sich, dass **Produktausbringung** ausgewählt ist, und klicken Sie dann auf **OK**.

3 Geben Sie einen Namen für den Task ein, den Sie erstellen möchten, und fügen Sie gegebenenfalls Anmerkungen hinzu.

4 Wählen Sie neben **Zielplattformen** die Typen der Plattform für die Ausbringung aus.

5 Legen Sie neben **Produkte und Komponenten** Folgendes fest:

   - Wählen Sie in der ersten Dropdown-Liste ein Produkt aus. Aufgeführt sind diejenigen Produkte, für die Sie bereits ein Paket in das Master-Repository eingecheckt haben. Wenn das bereitzustellende Produkt hier nicht aufgeführt ist, müssen Sie das Paket dieses Produkts einchecken.
   - Legen Sie als **Aktion** den Wert **Installieren** fest, und wählen Sie dann die **Sprache** des Pakets und den **Zweig** aus.
   - Geben Sie die Befehlszeilenoptionen für die Installation in das Textfeld **Befehlszeile** ein. Informationen zu Befehlszeilenoptionen des zu installierenden Produkts finden Sie in der Produktdokumentation.

   Sie können auf **+** oder **-** klicken, um Produkte und Komponenten zur angezeigten Liste hinzuzufügen bzw. daraus zu entfernen.

6 Wenn bereits bereitgestellte Sicherheitsprodukte automatisch aktualisiert werden sollen, wählen Sie **Automatische Aktualisierung** aus.

   Damit werden auch die HotFixes und Patches für die Produkte automatisch bereitgestellt.

   Wenn Sie die automatische Aktualisierung eines Sicherheitsprodukts festlegen, können Sie nicht die **Aktion** auf **Entfernen** festlegen.

7 Wählen Sie neben **Optionen** aus, ob dieser Task bei jedem Richtlinienerzwingungsvorgang ausgeführt werden soll (nur unter Windows), und klicken Sie dann auf **Speichern**.

8 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Systeme**, wählen Sie das System aus, auf dem ein Produkt ausgebracht werden soll, und klicken Sie dann auf **Aktionen** | **Agent** | **Tasks auf einem einzelnen System ändern**.

9 Klicken Sie auf **Aktionen** | **Neue Client-Task-Zuweisung**.

10 Wählen Sie auf der Seite **Task auswählen** unter **Produkt** den Eintrag **McAfee Agent** und unter **Task-Typ** den Eintrag **Produktausbringung** aus. Wählen Sie anschließend den Task aus, den Sie für die Ausbringung des Produkts erstellt haben.

11 Wählen Sie neben **Tags** die Plattformen aus, auf denen Sie die Pakete bereitstellen möchten, und klicken Sie dann auf **Weiter**:

- **Diesen Task an alle Computer senden**
- **Diesen Task nur an Computer senden, die die folgenden Kriterien erfüllen** – Klicken Sie neben dem zu konfigurierenden Kriterium auf **Bearbeiten**, wählen Sie die Tag-Gruppe sowie das für das Kriterium zu verwendende Tag aus, und klicken Sie anschließend auf **OK**.

Um die Liste auf bestimmte Tags zu beschränken, geben Sie den Tagnamen in das Textfeld unter **Tags** ein.

12 Wählen Sie auf der Seite Plan aus, ob die Planung aktiviert ist, geben Sie die Details für den Zeitplan an, und klicken Sie dann auf **Weiter**.

13 Überprüfen Sie die Zusammenfassung, und klicken Sie dann auf **Speichern**.

Aktualisierungs-Tasks

Wenn Sie die globale Aktualisierung nicht verwenden, legen Sie fest, wann Agenten auf verwalteten Systemen Aktualisierungen erhalten.

Sie können Aktualisierungs-Client-Tasks erstellen und festlegen, wann und wie die Aktualisierungspakete von den verwalteten Systemen abgerufen werden.

Bei Verwendung der globalen Aktualisierung ist dieser Task nicht erforderlich. Sie können dennoch zu Redundanzzwecken einen täglichen Task erstellen.

Erwägungen beim Erstellen von Aktualisierungs-Client-Tasks

Ziehen Sie beim Planen von Client-Aktualisierungs-Tasks Folgendes in Erwägung:

- Erstellen Sie täglich einen Aktualisierungs-Client-Task auf der obersten Ebene der Systemstruktur, damit der Task von allen Systemen geerbt wird. In großen Unternehmen sollten Sie Zufallsintervalle verwenden, damit weniger Bandbreite in Anspruch genommen wird. Bei großen Netzwerken mit Niederlassungen in verschiedenen Zeitzonen sollte der Task für die einzelnen verwalteten Systeme zur lokalen Systemzeit ausgeführt werden und nicht für alle Systeme gleichzeitig. Auf diese Weise erreichen Sie einen besseren Lastausgleich im Netzwerk.
- Wenn Sie geplante Replizierungs-Tasks verwenden, planen Sie den Task mindestens eine Stunde nach dem geplanten Replizierungs-Task.
- Führen Sie Aktualisierungs-Tasks für DAT- und Scan-Modul-Dateien mindestens einmal täglich aus. Verwaltete Systeme könnten beim Netzwerk abgemeldet sein und den geplanten Task verpassen. Durch häufiges Ausführen des Tasks stellen Sie sicher, dass auch diese Systeme die Aktualisierung erhalten.
- Maximieren Sie die Bandbreiteneffizienz, indem Sie verschiedene geplante Client-Aktualisierungs-Tasks erstellen, mit denen separate Komponenten aktualisiert werden und die zu unterschiedlichen Zeiten ausgeführt werden. So können Sie beispielsweise einen Task erstellen, mit dem nur DAT-Dateien aktualisiert werden, und einen weiteren Task, mit dem DAT- und Scan-Modul-Dateien wöchentlich oder monatlich aktualisiert werden (Scan-Modul-Pakete werden seltener veröffentlicht).

- Erstellen und planen Sie weitere Tasks zum Aktualisieren von Produkten, für die nicht McAfee Agent für Windows verwendet wird.
- Erstellen Sie einen Task zum Aktualisieren der wichtigsten Workstation-Anwendungen, um zu gewährleisten, dass alle Anwendungen die Aktualisierungsdateien erhalten. Planen Sie den Task so, dass dieser täglich oder mehrmals täglich ausgeführt wird.

Anzeigen eines zugewiesenen Client-Tasks

Bei der ersten Produktbereitstellung wird in ePolicy Orchestrator automatisch ein Client-Task für die Produktbereitstellung erstellt. Diesen zugewiesenen Client-Task können Sie als Grundlage verwenden, um weitere Client-Tasks zur Produktbereitstellung zu erstellen.

Bevor Sie beginnen

Es sind keine Standard-Client-Tasks zur Produktausbringung verfügbar. Führen Sie die erste Produktausbringung aus, um den Client-Task für die erste Produktausbringung zu erstellen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wenn Sie den Client-Task für die erste Produktausbringung anzeigen möchten, klicken Sie auf **Menü** | **Client-Task-Katalog**.
2. Wenn Sie den Client-Task der ersten Produktausbringung anzeigen möchten, wählen Sie in der Liste **Client-Task-Typen** die Option **McAfee Agent** | **Produktausbringung** aus.

   Für den als Erstes erstellten Client-Task zur Produktausbringung wird der Name der Gruppe **Systemstruktur** verwendet, den Sie in der **URL-Adresse für Agenten-Ausbringung** als InitialDeployment_<Gruppenname> konfiguriert haben. Zum Beispiel: "InitialDeployment_AlleWindowsSysteme" Dieser Task wird in der Tabelle **McAfee Agent** | **Produktausbringung** in der Spalte **Name** angezeigt.
3. Zum Öffnen des Client-Tasks doppelklicken Sie auf den Namen des Tasks, der unter **URL-Adresse für Agenten-Ausbringung** konfiguriert ist. Daraufhin werden die Client-Task-Details angezeigt.
4. Klicken Sie auf **Abbrechen**, um die Seite zu schließen.

Sie haben nun alle nötigen Informationen zum Speicherort und zur Konfiguration des standardmäßigen Client-Tasks zur Produktbereitstellung. Sie können diesen Client-Task auch duplizieren, um beispielsweise McAfee Agent auf Plattformen mit anderen Betriebssystemen bereitzustellen.

Regelmäßiges Aktualisieren von verwalteten Systemen mit einem geplanten Aktualisierungs-Task

Erstellen und konfigurieren Sie Aktualisierungs-Tasks. Wenn Sie die globale Aktualisierung verwenden, sollten Sie mithilfe eines täglichen Aktualisierungs-Client-Tasks sicherstellen, dass die DAT- und Moduldateien auf den Systemen auf dem aktuellen Stand sind.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Öffnen Sie das Dialogfeld Neuer Task.
   a. Wählen Sie die folgenden Optionen aus: **Menü** | **Richtlinie** | **Client-Task-Katalog**.
   b. Wählen Sie unter Client-Task-Typen ein Produkt aus.
   c. Klicken Sie auf **Neuer Task**.

2 Vergewissern Sie sich, dass **Produktaktualisierung** ausgewählt ist, und klicken Sie dann auf **OK**.

3 Geben Sie einen Namen für den Task ein, den Sie erstellen möchten, und fügen Sie gegebenenfalls Anmerkungen hinzu.

4 Wählen Sie neben dem Dialogfeld Aktualisierung wird ausgeführt aus, ob die Benutzer wissen sollen, dass eine Aktualisierung stattfindet, und ob sie den Vorgang aufschieben können.

5 Wählen Sie einen Pakettyp aus, und klicken Sie dann auf **Speichern**.

Wenn Sie beim Konfigurieren einzelner Signaturen und Module die Option **Modul** aktivieren und **DAT-Datei** deaktivieren, wird beim Aktualisieren des neuen Moduls auch die neue DAT-Datei automatisch aktualisiert, um den vollständigen Schutz sicherzustellen.

6 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Systeme**, wählen Sie dann das System aus, auf dem die Produktaktualisierung ausgebracht werden soll, und klicken Sie auf **Aktionen** | **Agent** | **Tasks auf einem einzelnen System ändern**.

7 Klicken Sie auf **Aktionen** | **Neue Client-Task-Zuweisung**.

8 Wählen Sie auf der Seite Task auswählen die folgenden Optionen aus:

- **Produkt**: Wählen Sie **McAfee Agent** aus.
- **Task-Typ**: Wählen Sie **Produktaktualisierung** aus.

Wählen Sie dann den Task aus, den Sie für die Ausbringung der Produktaktualisierung erstellt haben.

9 Wählen Sie neben Tags die Plattformen aus, auf denen Sie die Pakete bereitstellen möchten, und klicken Sie dann auf **Weiter**:

- **Diesen Task an alle Computer senden**
- **Diesen Task nur an Computer senden, die die folgenden Kriterien erfüllen** – Klicken Sie neben dem zu konfigurierenden Kriterium auf **Bearbeiten**, wählen Sie die Tag-Gruppe sowie das für das Kriterium zu verwendende Tag aus, und klicken Sie anschließend auf **OK**.

Um die Liste auf bestimmte Tags zu beschränken, geben Sie den Tagnamen in das Textfeld unter Tags ein.

10 Wählen Sie auf der Seite **Plan** aus, ob die Planung aktiviert ist, geben Sie die Details für den Zeitplan an, und klicken Sie dann auf **Weiter**.

11 Überprüfen Sie die Zusammenfassung, und klicken Sie dann auf **Speichern**.

Der Task wird der Liste der Client-Tasks für die Gruppen und Systeme hinzugefügt, auf die er angewendet wird. Agenten erhalten den neuen Aktualisierungs-Task bei der nächsten Kommunikation mit dem Server. Nach der Aktivierung wird der Task zum nächsten geplanten Zeitpunkt ausgeführt.

Jedes System wird abhängig von der Konfiguration der Richtlinien für den Agent dieses Clients aus dem entsprechenden Repository aktualisiert.

Testen neuer DAT-Dateien und Scan-Module vor dem Verteilen

Es ist sinnvoll, die DAT- und Scan-Modul-Dateien vor dem Ausbringen im gesamten Unternehmen auf einigen wenigen Systemen zu testen. Sie können Aktualisierungspakete mithilfe des Zweigs Test Ihres Master-Repositorys testen.

ePolicy Orchestrator stellt zu diesem Zweck drei Repository-Zweige zur Verfügung.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Erstellen Sie einen geplanten Repository-Abruf-Task, der Aktualisierungspakete in den Zweig Test des Master-Repositorys kopiert. Planen Sie ihn so, dass er nach der Veröffentlichung neuer DAT-Dateien durch McAfee ausgeführt wird.
2. Erstellen Sie eine Gruppe, oder wählen Sie in der Systemstruktur eine Gruppe aus, die als Testgruppe dienen soll, und erstellen Sie dann eine McAfee Agent-Richtlinie, nach der die Systeme nur den Zweig Test verwenden sollen (im Abschnitt **Repository-Zweig, der für die jeweiligen Aktualisierungstypen verwendet werden soll** auf der Registerkarte **Aktualisierungen**).

   Die Richtlinien werden wirksam, sobald der McAfee Agent den Server kontaktiert. Bei der nächsten Aktualisierung ruft der Agent die Aktualisierungen aus dem Zweig Test ab.
3. Erstellen Sie einen geplanten Client-Aktualisierungs-Task für die Testsysteme, der DAT- und Scan-Modul-Dateien aus dem Zweig Test des Repositorys aktualisiert. Planen Sie den Task so, dass er ein oder zwei Stunden nach dem geplanten Beginn des Repository-Abruf-Tasks ausgeführt wird.

   Der erstellte Aktualisierungs-Task zum Testen auf der Ebene der Testgruppe sorgt dafür, dass er nur für diese Gruppe ausgeführt wird.
4. Überwachen Sie die Systeme in der Testgruppe so lange, bis Sie mit dem Ergebnis zufrieden sind.
5. Verschieben Sie die Pakete aus dem Zweig Test in den Zweig Aktuell Ihres Master-Repositorys. Klicken Sie auf **Menü** | **Software** | **Master-Repository**, um die Seite **Master-Repository** zu öffnen.

   Durch Hinzufügen zum Zweig Aktuell stehen die Pakete nun Ihrer Produktionsumgebung zur Verfügung. Wenn das nächste Mal ein Client-Aktualisierungs-Task Pakete aus dem Zweig Aktuell abruft, werden die neuen DAT- und Scan-Modul-Dateien an die Systeme verteilt, die den Task verwenden.

Verwalten von Client-Tasks

Sie können Client-Tasks erstellen und verwalten.

Aufgaben

- *Erstellen von Client-Tasks* auf Seite 241
  Verwenden Sie Client-Tasks, um automatische Produktaktualisierungen auszuführen. Dieser Vorgang ist für alle Client-Tasks ähnlich.
- *Bearbeiten von Client-Tasks* auf Seite 242
  Sie können alle zuvor konfigurierten Client-Task-Einstellungen oder Zeitplaninformationen bearbeiten.
- *Löschen von Client-Tasks* auf Seite 242
  Sie können jeden zuvor konfigurierten Client-Task löschen.
- *Vergleichen von Client-Tasks* auf Seite 243
  Mit dem Tool **Client-Task-Vergleich** können Sie ähnliche Client-Tasks vergleichen. Auf diese Weise können Sie ermitteln, welche Einstellungen sich unterscheiden und welche identisch sind.

Erstellen von Client-Tasks

Verwenden Sie Client-Tasks, um automatische Produktaktualisierungen auszuführen. Dieser Vorgang ist für alle Client-Tasks ähnlich.

In einigen Fällen müssen Sie eine neue Client-Task-Zuweisung erstellen, um einen Client-Task einer Systemstrukturgruppe zuzuordnen.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Öffnen Sie das Dialogfeld Neuer Task.

   a Wählen Sie die folgenden Optionen aus: **Menü** | **Richtlinie** | **Client-Task-Katalog**.

   b Wählen Sie unter Client-Task-Typen ein Produkt aus.

   c Klicken Sie auf **Neuer Task**.

2 Wählen Sie einen Task-Typ aus der Liste aus, und klicken Sie dann auf **OK**.

   Der Generator für Client-Tasks wird geöffnet.

3 Geben Sie einen Namen für den Task ein, fügen Sie eine Beschreibung hinzu, und konfigurieren Sie dann die Einstellungen für den bestimmten Task-Typ, den Sie erstellen.

   Welche Konfigurationsoptionen zur Verfügung stehen, hängt vom ausgewählten Task-Typ ab.

4 Überprüfen Sie die Task-Einstellungen, und klicken Sie dann auf **Speichern**.

Der Task wird der Liste der Client-Tasks für den ausgewählten Client-Task-Typ hinzugefügt.

Bearbeiten von Client-Tasks

Sie können alle zuvor konfigurierten Client-Task-Einstellungen oder Zeitplaninformationen bearbeiten.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Richtlinie** | **Client-Task-Katalog**. Das Dialogfeld **Client-Task-Katalog** wird angezeigt.

2 Wählen Sie links in der Navigationsstruktur den **Client-Task-Typ** aus. Die verfügbaren Client-Tasks werden rechts im Fenster angezeigt.

3 Doppelklicken Sie auf den Namen des Client-Tasks. Das Dialogfeld **Client-Task-Katalog** wird mit dem Client-Task angezeigt.

4 Bearbeiten Sie die Task-Einstellungen nach Bedarf, und klicken Sie dann auf **Speichern**.

Die Änderungen werden auf den verwalteten Systemen nach der nächsten Agent-zu-Server-Kommunikation wirksam.

Löschen von Client-Tasks

Sie können jeden zuvor konfigurierten Client-Task löschen.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Richtlinie** | **Client-Task-Katalog**. Das Dialogfeld **Client-Task-Katalog** wird angezeigt.

2 Wählen Sie links in der Navigationsstruktur den **Client-Task-Typ** aus. Die verfügbaren Client-Tasks werden rechts im Fenster angezeigt.

3 Klicken Sie in der Spalte **Aktionen** neben dem gewünschten Client-Task auf **Löschen**.

4 Klicken Sie auf **OK**.

Vergleichen von Client-Tasks

Mit dem Tool **Client-Task-Vergleich** können Sie ähnliche Client-Tasks vergleichen. Auf diese Weise können Sie ermitteln, welche Einstellungen sich unterscheiden und welche identisch sind.

Viele der auf dieser Seite enthaltenen Werte und Variablen sind produktspezifisch. Informationen zu Optionen, die nicht in der nachfolgenden Tabelle aufgeführt sind, finden Sie in der Produktdokumentation des jeweiligen Produkts, von dem der zu vergleichende Client-Task stammt.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Client-Task-Vergleich**, wählen Sie ein **Produkt** und einen **Client-Task-Typ** aus, und wählen Sie für die Einstellungen in den Listen die Option **Anzeigen** aus.

   Mit diesen Einstellungen werden die zu vergleichenden Client-Tasks in den Listen **Client-Task 1** und **Client-Task 2** aufgefüllt.

2 Wählen Sie in der Zeile **Client-Tasks vergleichen** in den Spalten **Client-Task 1** und **Client-Task 2** die zu vergleichenden Client-Tasks aus.

   In den beiden oberen Zeilen der Tabelle wird die Anzahl der abweichenden bzw. identischen Einstellungen angezeigt. Sie können auch weniger Daten anzeigen, indem Sie die Einstellung **Anzeigen** von **Alle Client-Task-Einstellungen** in **Unterschiede zwischen Client-Tasks** und **Übereinstimmungen zwischen Client-Tasks** ändern.

3 Klicken Sie auf **Drucken**, um eine druckfähige Ansicht des Vergleichs anzuzeigen.

18 Server-Tasks

Server-Tasks sind konfigurierbare Aktionen, die zu geplanten Zeiten oder in geplanten Intervallen auf McAfee ePO ausgeführt werden. Nutzen Sie Server-Tasks, um sich wiederholende Tasks zu automatisieren.

McAfee ePO enthält vorkonfigurierte Server-Tasks und Aktionen. Mit vielen zusätzlichen Software-Produkten, die mit McAfee ePO verwaltet werden, werden weitere vorkonfigurierte Server-Tasks hinzugefügt.

Inhalt

- *Erstellen eines Server-Tasks*
- *Zulässige Cron-Syntax beim Planen von Server-Tasks*
- *Das Server-Task-Protokoll*

Erstellen eines Server-Tasks

Erstellen Sie Server-Tasks, um die Ausführung verschiedener Aktionen nach einer angegebenen Planung zu planen.

Wenn Sie in McAfee ePO bestimmte Aktionen ohne manuelles Eingreifen ausführen möchten, nutzen Sie am besten einen Server-Task.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Automatisierung** | **Server-Tasks** und dann auf **Aktionen** | **Neuer Task**.

Der Generator für Client-Tasks wird mit der Seite Beschreibung geöffnet.

2 Geben Sie dem Task einen geeigneten Namen, und entscheiden Sie, ob der Task einen Planungsstatus besitzt. Klicken Sie auf **Weiter**.

Wenn der Task automatisch ausgeführt werden soll, legen Sie den **Planungsstatus** auf **Aktiviert** fest.

Daraufhin wird die Seite Aktionen angezeigt.

3 Wählen Sie die Aktion für den Task aus, und konfigurieren Sie diese. Klicken Sie dann auf **Weiter**.

Die Seite Plan wird angezeigt.

4 Wählen Sie den Planungstyp (die Häufigkeit), das Startdatum, das Enddatum und die Uhrzeit für die Ausführung des Tasks aus. Klicken Sie auf **Weiter**.

Diese Planungsinformationen kommen nur zum Einsatz, wenn Sie die Option **Planungsstatus** aktivieren.

Daraufhin wird die Seite Zusammenfassung angezeigt.

5 Klicken Sie auf **Speichern**, um den Server-Task zu speichern.

Der neue Task wird in der Liste Server-Tasks angezeigt.

Zulässige Cron-Syntax beim Planen von Server-Tasks

Wenn Sie bei der Planung eines Server-Tasks die Option **Erweitert** auswählen, können Sie eine Planung mit Cron-Syntax angeben.

Die Cron-Syntax besteht aus sechs oder sieben Feldern, getrennt durch ein Leerzeichen. Die zulässige Cron-Syntax ist, nach Feldern in absteigender Reihenfolge, in der folgenden Tabelle aufgeführt. Die meisten Cron-Syntaxen sind zulässig, einige wenige Fälle werden jedoch nicht unterstützt. Sie können beispielsweise nicht gleichzeitig Werte für den Wochentag und den Tag des Monats angeben.

Feldname	Zulässige Werte	Zulässige Sonderzeichen
Sekunden	0–59	, - * /
Minuten	0–59	, - * /
Stunden	0–23	, - * /
Tag des Monats	1–31	, - * ? / L W C
Monat	1–12 oder JAN – DEC	, - * /
Wochentag	1–7 oder SUN – SAT	, - * ? / L C #
Jahr (optional)	Leer oder 1970–2099	, - * /

Zulässige Sonderzeichen

- Kommas (,) sind zulässig, um weitere Werte anzugeben. Beispiel: "`5,10,30`" oder "`MON,WED,FRI`".
- Sternchen (*) werden für die Angabe "jede" verwendet. So bedeutet zum Beispiel "`*`" im Feld **Minuten** "jede Minute".
- Fragezeichen (?) sind zulässig, um keinen spezifischen Wert für den Wochentag oder den Tag im Monat anzugeben.

  Sie müssen das Fragezeichen in einem der Felder verwenden, können es jedoch nicht gleichzeitig in beiden Feldern verwenden.

- Schrägstriche (/) kennzeichnen Inkremente. So bedeutet zum Beispiel "`5/15`" im Feld **Minuten**, dass der Task in der 5., 20., 35. und 50. Minute ausgeführt wird.
- Der Buchstabe "L" bedeutet "letzter" in den Feldern **Wochentag** und **Tag des Monats**. So bedeutet zum Beispiel "`0 15 10 ? * 6L`": der letzte Freitag jeden Monats um 10:15 Uhr.
- Der Buchstabe "W" steht für "Wochentag". Wenn Sie also als Tag des Monats "`15W`" erstellt haben, bezeichnet dies den Wochentag, der dem 15. des Monats am nächsten liegt. Sie können auch "`LW`" angeben, was für den letzten Wochentag des Monats steht.
- Das Rautenzeichen "#" kennzeichnet den "n-ten" Tag des Monats. So steht zum Beispiel "`6#3`" im Feld **Wochentag** für den dritten Freitag jeden Monats, "`2#1`" für den ersten Montag und "`4#5`" für den fünften Mittwoch.

  Wenn es im jeweiligen Monat keinen fünften Mittwoch gibt, wird der Task nicht ausgeführt.

Das Server-Task-Protokoll

Im Server-Task-Protokoll können Sie die detaillierten Ergebnisse geplanter Server-Tasks anzeigen, die auf dem Server ausgeführt wurden oder werden.

Einträge in dem Protokoll enthalten Einzelheiten zu den folgenden Punkten:

- Erfolg oder Fehler des Tasks
- Alle Sub-Tasks, die während der Ausführung des geplanten Tasks ausgeführt wurden

Sie können einen Task, der gerade ausgeführt wird, auch abbrechen.

Anzeigen von Informationen zu Server-Tasks im Server-Task-Protokoll

Überprüfen Sie das Server-Task-Protokoll auf Informationen zu Server-Tasks. Dem Server-Task-Protokoll können Sie den Status des jeweiligen Tasks und eventuell aufgetretene Fehler entnehmen.

- Greifen Sie auf Informationen zu Server-Tasks zu: Klicken Sie auf **Menü** | **Automatisierung** | **Server-Task-Protokoll**.

Die folgenden Task-Informationen werden angezeigt:

- Startdatum und Task-Dauer
- Fehler oder Warnungen und die zugehörigen Codes
- Status der einzelnen Pakete, die in das Master-Repository eingecheckt werden
- Informationen zu neuen Paketen, die in das Master-Repository eingecheckt werden
- Task-Status für jede Site (wenn erweitert)
- Eventuelle Fehler und Warnungen (und deren Codes) und für welche Site sie gelten

Verwalten des Server-Task-Protokolls

Nachdem Sie das Server-Task-Protokoll geöffnet haben, können Sie die Task-Protokolle je nach Bedarf anzeigen, filtern und bereinigen.

Der Status jedes Server-Tasks wird in der Spalte **Status** angezeigt:

- **Wartet** – Der Task wartet darauf, dass ein anderer Task abgeschlossen wird.
- **Wird ausgeführt** – Der Task wurde gestartet, aber noch nicht abgeschlossen.
- **Pausiert** – Der Task wurde durch eine Server-Task-Aktion pausiert.
- **Angehalten** – Der Task wurde durch eine Server-Task-Aktion angehalten.
- **Fehlgeschlagen** – Der Task wurde gestartet, aber nicht erfolgreich abgeschlossen.
- **Abgeschlossen** – Der Task wurde erfolgreich abgeschlossen.
- **Ausstehende Beendigung** – Eine Beendigungsanforderung wurde gesendet.
- **Beendet** – Der Task wurde vor seinem Abschluss manuell beendet.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Automatisierung** | **Server-Task-Protokoll**. Die Seite Server-Task-Protokoll wird angezeigt.

2 Wählen Sie eine der folgenden Aktionen aus:

Aktion	Vorgehensweise
Anzeigen des Server-Task-Protokolls	1 Klicken Sie auf einen Spaltentitel, um die Ereignisse zu sortieren. 2 Wählen Sie eines der Task-Protokolle aus, klicken Sie auf **Aktionen**, und wählen Sie eine der folgenden Optionen zum Ändern des Server-Task-Protokolls aus: • **Spalten auswählen** – Die Seite **Spalten zum Anzeigen auswählen** wird angezeigt. • **Tabelle exportieren** – Die Seite **Exportieren** wird angezeigt. • **Bereinigen**: Das Dialogfeld **Bereinigen** wird angezeigt. Geben Sie mit einer Zahl und einer Zeiteinheit an, welche Task-Protokolleinträge gelöscht werden sollen, und klicken Sie dann auf **OK**. • **Task beenden** – Beendet einen Task, der gerade ausgeführt wird.
Filtern des Server-Task-Protokolls	Wählen Sie in der Dropdown-Liste **Filter** einen Filter aus.
Bereinigen des Server-Task-Protokolls	1 Klicken Sie auf **Aktionen**	**Bereinigen**. 2 Geben Sie im Dialogfeld **Bereinigen** eine Anzahl von Tagen, Wochen, Monaten oder Jahren ein. Alle Elemente, die mindestens so alt sind, werden gelöscht. 3 Klicken Sie auf **OK**.

19 Verwalten von SQL-Datenbanken

Sie können SQL Server-Datenbanken sichern, wiederherstellen, warten und verwalten.

Inhalt

- *Warten von SQL-Datenbanken*
- *Ermitteln des Servers und des Namens der Microsoft SQL-Datenbank mithilfe eines Remote-Befehls*
- *Konfigurieren eines Snapshots und Wiederherstellen der SQL-Datenbank*
- *Ermitteln des Servers und des Namens der Microsoft SQL-Datenbank mithilfe eines Remote-Befehls*
- *Ermitteln von Informationen über den McAfee ePO-Server mithilfe von Microsoft SQL Server Management Studio*
- *Das Bedrohungsereignisprotokoll*

Warten von SQL-Datenbanken

Sie müssen die ePolicy Orchestrator-Datenbanken regelmäßig warten, um die optimale Leistung und den Schutz der Daten sicherzustellen.

Verwenden Sie dazu das Microsoft-Verwaltungs-Tool für die jeweilige SQL Server-Version:

SQL Server-Version	Verwaltungs-Tool
SQL Server 2008 und SQL Server 2012	SQL Server Management Studio
SQL Server Express	SQL Server Management Studio Express

Je nach der Bereitstellung von ePolicy Orchestrator sollten Sie wöchentlich einige Stunden für reguläre Datenbanksicherungen und Wartungs-Tasks einplanen. Die Tasks sollten regelmäßig (entweder wöchentlich oder täglich) ausgeführt werden. Dies sind jedoch nicht die einzigen Wartungs-Tasks, die zur Verfügung stehen. Weitere Informationen zu Wartungsoptionen finden Sie in Ihrer SQL Server-Dokumentation.

Ermitteln des Servers und des Namens der Microsoft SQL-Datenbank mithilfe eines Remote-Befehls

Mit dem folgenden Remote-Befehl von ePolicy Orchestrator können Sie den Server und den Namen der Microsoft SQL-Datenbank ermitteln.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Geben Sie den folgenden Remote-Befehl in die Adresszeile eines Web-Browsers ein:

```
https://localhost:8443/core/config
```

Die einzelnen Parameter bedeuten Folgendes:

- `localhost` – Der Name Ihres McAfee ePO-Servers.
- `:8443` – Der Standardport des McAfee ePO-Servers. Ihr Server kann auch für die Verwendung einer anderen Portnummer konfiguriert sein.

2 Speichern Sie die folgenden Informationen, die auf der Seite **Datenbankeinstellungen konfigurieren** angezeigt werden:

- Hostname oder IP-Adresse
- Datenbankname

Konfigurieren eines Snapshots und Wiederherstellen der SQL-Datenbank

Für eine schnelle Neuinstallation eines McAfee ePO-Servers müssen Sie einen Snapshot für die Wiederherstellung nach einem Systemausfall konfigurieren und speichern, oder sicherstellen, dass ein Snapshot in der SQL-Datenbank gespeichert wird. Anschließend erstellen Sie eine Sicherung der SQL-Datenbank, in der sich der Snapshot befindet, und kopieren die Datenbank-Sicherungsdatei auf einen SQL-Wiederherstellungs-Server.

Für eine schnelle Neuinstallation eines McAfee ePO-Servers müssen Sie folgende Aufgaben ausführen.

Aufgaben

- *Konfigurieren eines Tasks zur Erstellung eines Server-Snapshots für die Wiederherstellung nach einem Systemausfall* auf Seite 250
  Mithilfe des Tasks "Server-Snapshot für Wiederherstellung nach Systemausfall" können Sie die geplanten automatischen Snapshots einer McAfee ePO-Server-Konfiguration ändern, die in der SQL-Datenbank gespeichert sind.
- *Sichern und Wiederherstellen von Datenbanken mithilfe von Microsoft SQL Server* auf Seite 251
  Verwenden Sie die Prozeduren von Microsoft SQL Server zum Speichern des Snapshots für die Wiederherstellung nach einem Systemausfall, in dem sich die Konfigurationsinformationen des McAfee ePO-Servers befinden.

Konfigurieren eines Tasks zur Erstellung eines Server-Snapshots für die Wiederherstellung nach einem Systemausfall

Mithilfe des Tasks "Server-Snapshot für Wiederherstellung nach Systemausfall" können Sie die geplanten automatischen Snapshots einer McAfee ePO-Server-Konfiguration ändern, die in der SQL-Datenbank gespeichert sind.

Der vorkonfigurierte Status eines Tasks "Server-Snapshot für Wiederherstellung nach Systemausfall" hängt von der SQL-Datenbank ab, die der McAfee ePO-Server verwendet. Bei allen Editionen von Microsoft SQL Server (außer der Express Edition) ist die Snapshot-Funktion für die Wiederherstellung nach einem Systemausfall standardmäßig aktiviert.

Aufgrund der Größenbeschränkungen bei Datendateien in Microsoft SQL Server Express Edition rät McAfee davon ab, die Planung von Snapshots für die Wiederherstellung nach einem Systemausfall zu aktivieren. Bei Microsoft SQL Server 2005 Express Edition beträgt die maximale Dateigröße nur 4 GB und bei Microsoft SQL Server 2008 Express Edition sowie Microsoft SQL Server 2012 Express Edition nur 10 GB.

Es kann immer nur ein Snapshot für die Wiederherstellung nach einem Systemausfall ausgeführt werden. Wenn Sie mehrere Snapshots ausführen, erstellt nur der letzte Snapshot eine Ausgabe, wobei die vorherigen Snapshots überschrieben werden.

Je nach Bedarf können Sie den standardmäßigen Task zur Erstellung eines Server-Snapshots für die Wiederherstellung nach einem Systemausfall ändern.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Server-Tasks**, wählen Sie in der Liste **Server-Tasks** den Eintrag **Server-Snapshot für Wiederherstellung nach Systemausfall** aus, und klicken Sie auf **Bearbeiten**.

   Der Assistent für Tasks zur Erstellung eines Server-Snapshots für die Wiederherstellung nach einem Systemausfall wird angezeigt.

2 Klicken Sie auf der Registerkarte **Beschreibungen** unter **Planungsstatus** je nach Bedarf auf **Aktiviert** oder **Deaktiviert**.

3 Ändern Sie auf der Registerkarte **Plan** je nach Bedarf die folgenden Einstellungen:

   - **Planungstyp** – Legt fest, wie häufig der Snapshot gespeichert wird.
   - **Startdatum** und **Enddatum** – Legen Sie das Start- und Enddatum zum Speichern der Snapshots fest, oder klicken Sie auf **Kein Enddatum**, wenn der Task dauerhaft ausgeführt werden soll.
   - **Plan** – Hiermit legen Sie die Uhrzeit fest, zu der der Snapshot gespeichert werden soll. In der Standardeinstellung wird der Snapshot-Task jeden Tag um 01:59 Uhr ausgeführt.

   McAfee empfiehlt, den Task zur Erstellung eines Server-Snapshots für die Wiederherstellung nach einem Systemausfall außerhalb der Spitzenzeiten auszuführen, damit während der Erstellung des Snapshots möglichst wenige Änderungen an der Datenbank vorgenommen werden.

4 Überprüfen Sie auf der Registerkarte **Zusammenfassung**, dass der Server-Task ordnungsgemäß konfiguriert ist, und klicken Sie dann auf **Speichern**.

Sichern und Wiederherstellen von Datenbanken mithilfe von Microsoft SQL Server

Verwenden Sie die Prozeduren von Microsoft SQL Server zum Speichern des Snapshots für die Wiederherstellung nach einem Systemausfall, in dem sich die Konfigurationsinformationen des McAfee ePO-Servers befinden.

Bevor Sie beginnen

Hierfür müssen Sie über Konnektivität sowie über eine Autorisierung verfügen, um Dateien vom primären auf den McAfee ePO-SQL-Wiederherstellungs-Server kopieren zu können. Ausführliche Informationen dazu finden Sie in *Anhang A: Verwalten von ePolicy Orchestrator-Datenbanken*.

Nachdem Sie einen Snapshot der Konfiguration des McAfee ePO-Servers erstellt haben, führen Sie folgende Aktionen durch:

Vorgehensweise

1 Erstellen Sie eine Microsoft SQL Server-Sicherung der Datenbank mithilfe von:

   - Microsoft SQL Server Management Studio
   - Microsoft Transact-SQL

   Ausführliche Informationen zur Durchführung dieser Prozesse finden Sie in der Dokumentation von Microsoft SQL Server.

2 Kopieren Sie die erstellte Sicherungsdatei auf den SQL-Wiederherstellungs-Server.

3 Stellen Sie die Sicherung der primären SQL-Datenbank wieder her, in der sich die Snapshot-Datensätze für die Wiederherstellung nach einem Systemausfall befinden. Verwenden Sie dazu:

- Microsoft SQL Server Management Studio
- Microsoft Transact-SQL

Ausführliche Informationen zur Durchführung dieser Prozesse finden Sie in der Dokumentation von Microsoft SQL Server.

Dadurch wird ein SQL-Server-Duplikat erstellt, das bei Bedarf wiederhergestellt werden kann. Dazu wird es bei einer Neuinstallation von ePolicy Orchestrator mit der Option **Wiederherstellen** eingebunden.

Ermitteln des Servers und des Namens der Microsoft SQL-Datenbank mithilfe eines Remote-Befehls

Mit dem folgenden Remote-Befehl von ePolicy Orchestrator können Sie den Server und den Namen der Microsoft SQL-Datenbank ermitteln.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Geben Sie den folgenden Remote-Befehl in die Adresszeile eines Web-Browsers ein:

```
https://localhost:8443/core/config
```

Die einzelnen Parameter bedeuten Folgendes:

- `localhost` – Der Name Ihres McAfee ePO-Servers.
- `:8443` – Der Standardport des McAfee ePO-Servers. Ihr Server kann auch für die Verwendung einer anderen Portnummer konfiguriert sein.

2 Speichern Sie die folgenden Informationen, die auf der Seite **Datenbankeinstellungen konfigurieren** angezeigt werden:

- Hostname oder IP-Adresse
- Datenbankname

Ermitteln von Informationen über den McAfee ePO-Server mithilfe von Microsoft SQL Server Management Studio

Ermitteln Sie in Microsoft SQL Server Management Studio Informationen zu Ihrem vorhandenen McAfee ePO-Server.

Vorgehensweise

1 Melden Sie sich mittels Remote-Desktopverbindung bei dem Hostnamen oder der IP-Adresse des Microsoft SQL-Datenbank-Servers an.

2 Öffnen Sie Microsoft SQL Server Management Studio, und stellen Sie eine Verbindung zum SQL-Server her.

3 Klicken Sie in der Liste **Objekt-Explorer** auf **<Name des Datenbank-Servers>** | **Datenbanken** | **<Datenbankname>** | **Tabellen**.

4 Führen Sie einen Bildlauf durch, bis Sie die Tabelle **EPOServerInfo** finden. Klicken Sie dann mit der rechten Maustaste auf den Tabellennamen, und wählen Sie in der Liste den Eintrag **Oberste 200 Zeilen bearbeiten** aus.

5 Suchen Sie die Informationen in den folgenden Datensätzen, und speichern Sie sie.

- **ePOVersion** – Zum Beispiel 5.1.0
- **DNSName** – Zum Beispiel epo-2k8-epo51.server.com
- **ComputerName** – Zum Beispiel EPO-2K8-EPO51
- **LastKnownTCPIP** – Zum Beispiel 172.10.10.10
- **RmdSecureHttpPort** – Zum Beispiel 8443

Notieren Sie sich diese Informationen. Falls Sie ePolicy Orchestrator wiederherstellen müssen, benötigen Sie diese Angaben.

Das Bedrohungsereignisprotokoll

Mithilfe des Bedrohungsereignisprotokolls können Sie Ereignisse in der Datenbank schnell anzeigen und sortieren. Das Protokoll kann nur nach Alter bereinigt werden.

Sie können wählen, welche Spalten in der sortierbaren Tabelle angezeigt werden sollen. Es steht eine Vielzahl von Ereignisdaten als Spalten zur Auswahl.

Je nach den verwalteten Produkten können Sie auch mit bestimmten Aktionen auf die Ereignisse reagieren. Aktionen sind im Menü **Aktionen** unten auf der Seite verfügbar.

Einheitliches Ereignisformat

In den meisten verwalteten Produkten kommt nun ein einheitliches Ereignisformat zum Einsatz. Die Felder dieses Formats können als Spalten im Bedrohungsereignisprotokoll verwendet werden. Dazu gehören:

- **Ausgeführte Aktion** – Die Aktion, die vom Produkt als Reaktion auf die Bedrohung ausgeführt wurde.
- **Agenten-GUID** – Die eindeutige Kennung des Agenten, von dem das Ereignis weitergeleitet wurde.
- **DAT-Version** – Die DAT-Version auf dem System, von dem das Ereignis gesendet wurde.
- **Hostname des entdeckenden Produkts** – Der Name des Systems, auf dem das entdeckende Produkt gehostet ist.
- **ID des entdeckenden Produkts** – Die ID des entdeckenden Produkts.
- **IPv4-Adresse des entdeckenden Produkts** – Die IPv4-Adresse des Systems, auf dem das entdeckende Produkt gehostet ist (sofern zutreffend).
- **IPv6-Adresse des entdeckenden Produkts** – Die IPv6-Adresse des Systems, auf dem das entdeckende Produkt gehostet ist (sofern zutreffend).
- **MAC-Adresse des entdeckenden Produkts** – Die MAC-Adresse des Systems, auf dem das entdeckende Produkt gehostet ist.
- **Name des entdeckenden Produkts** – Der Name des entdeckenden Produkts, das verwaltet wird.
- **Version des entdeckenden Produkts** – Die Versionsnummer des entdeckenden Produkts.

- **Scan-Modul-Version** – Die Versionsnummer des Scan-Moduls des entdeckenden Produkts (sofern zutreffend).
- **Ereigniskategorie** – Die Kategorie des Ereignisses. Die mögliche Kategorien hängen vom Produkt ab.
- **Zeit der Ereignisgenerierung (UTC)** – Der Zeitpunkt, zu dem das Ereignis entdeckt wurde (in koordinierter Weltzeit).
- **Ereignis-ID** – Die eindeutige Kennung des Ereignisses.
- **Zeit des Ereignisempfangs (UTC)** – Der Zeitpunkt, zu dem das Ereignis vom McAfee ePO-Server empfangen wurde (in koordinierter Weltzeit).
- **Dateipfad** – Der Dateipfad des Systems, von dem das Ereignis gesendet wurde.
- **Hostname** – Der Name des Systems, von dem das Ereignis gesendet wurde.
- **IPv4-Adresse** – Die IPv4-Adresse des Systems, von dem das Ereignis gesendet wurde.
- **IPv6-Adresse** – Die IPv6-Adresse des Systems, von dem das Ereignis gesendet wurde.
- **MAC-Adresse** – Die MAC-Adresse des Systems, von dem das Ereignis gesendet wurde.
- **Netzwerkprotokoll** – Das Bedrohungszielprotokoll bei Netzwerk-Bedrohungsklassen.
- **Portnummer** – Der Bedrohungszielport bei Netzwerk-Bedrohungsklassen.
- **Prozessname** – Der Name des Zielprozesses (sofern zutreffend).
- **Server-ID** – Die ID des Servers, von dem das Ereignis gesendet wurde.
- **Name der Bedrohung** – Der Name der Bedrohung.
- **Hostname der Bedrohungsquelle** – Der Name des Systems, von dem die Bedrohung stammt.
- **IPv4-Adresse der Bedrohungsquelle** – Die IPv4-Adresse des Systems, von dem die Bedrohung stammt.
- **IPv6-Adresse der Bedrohungsquelle** – Die IPv6-Adresse des Systems, von dem die Bedrohung stammt.
- **MAC-Adresse der Bedrohungsquelle** – Die MAC-Adresse des Systems, von dem die Bedrohung stammt.
- **URL der Bedrohungsquelle** – Der URL des Systems, von dem die Bedrohung stammt.
- **Benutzername der Bedrohungsquelle** – Der Name des Benutzers, von dem die Bedrohung stammt.
- **Typ der Bedrohung** – Die Klasse der Bedrohung.
- **Benutzername** – Der Benutzername oder die E-Mail-Adresse der Bedrohungsquelle.

Anzeigen und Bereinigen des Bedrohungsereignisprotokolls

Sie sollten Ihre Bedrohungsereignisse in regelmäßigen Abständen anzeigen und bereinigen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Berichterstellung** | **Bedrohungsereignisprotokoll**.

2 Wählen Sie eine der folgenden Aktionen aus.

Aktion	Vorgehensweise
Anzeigen des Bedrohungsereignisprotokolls	1 Klicken Sie auf einen Spaltentitel, um die Ereignisse zu sortieren. Sie können auch auf **Aktionen** | **Spalten auswählen** klicken. Daraufhin wird die Seite **Spalten zum Anzeigen auswählen** angezeigt. 2 Wählen Sie in der Liste **Verfügbare Spalten** die Tabellenspalten aus, die Sie benötigen, und klicken Sie dann auf **Speichern**. 3 Wählen Sie Ereignisse in der Tabelle aus, klicken Sie dann auf **Aktionen**, und wählen Sie **Verwandte Systeme anzeigen** aus, um die Details der Systeme anzuzeigen, die die ausgewählten Ereignisse gesendet haben.
Bereinigen von Bedrohungsereignissen	1 Klicken Sie auf **Aktionen** | **Bereinigen**. 2 Geben Sie im Dialogfeld **Bereinigen** neben **Datensätze bereinigen, die älter sind als** eine Zahl ein, und wählen Sie eine Zeiteinheit aus. 3 Klicken Sie auf **OK**. Datensätze, die das angegebene Alter überschritten haben, werden dauerhaft gelöscht.

Planen der Bereinigung des Bedrohungsereignisprotokolls

Sie können einen Server-Task erstellen, mit dem das Bedrohungsereignisprotokoll automatisch bereinigt wird.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Öffnen Sie den **Generator für Server-Tasks**.
   a Wählen Sie die folgenden Optionen aus: **Menü** | **Automatisierung** | **Server-Tasks**.
   b Klicken Sie auf **Neuer Task**.
2 Geben Sie einen Namen und eine Beschreibung für den Task ein. Wählen Sie neben Planungsstatus die Option **Aktiviert** aus, und klicken Sie dann auf **Weiter**.
3 Wählen Sie in der Dropdown-Liste die Option **Bedrohungsereignisprotokoll bereinigen** aus.
4 Legen Sie fest, ob nach Alter oder anhand von Abfrageergebnissen bereinigt werden soll. Wenn Sie nach Abfrage bereinigen, müssen Sie eine Abfrage auswählen, deren Ergebnis eine Tabelle mit Ereignissen ist.
5 Klicken Sie auf **Weiter**.
6 Planen Sie den Task nach Bedarf, und klicken Sie dann auf **Weiter**.
7 Überprüfen Sie die Task-Details, und klicken Sie dann auf **Speichern**.

Überwachung und Berichterstellung zum Netzwerk-Sicherheitsstatus

Mithilfe anpassbarer Dashboards können Sie wichtige Sicherheitszustände auf einen Blick überwachen und diesen Status in vorkonfigurierten, anpassbaren Abfragen und Berichten an relevante Mitarbeiter und Entscheidungsträger melden.

Kapitel 20 *Dashboards und Monitore*
Kapitel 21 *Abfragen und Berichte*
Kapitel 22 *Ereignisse und Antworten*
Kapitel 23 *Probleme*
Kapitel 24 *Wiederherstellung nach Systemausfall*

20 Dashboards und Monitore

Mithilfe von Dashboards können Sie eine Umgebung ständig überwachen.

Dashboards sind Sammlungen von Monitoren. In Monitoren werden Informationen zu einer Umgebung in übersichtlichen Diagrammen zusammengefasst. In der Regel werden verwandte Monitore in einem bestimmten Dashboard gruppiert. Das Dashboard Bedrohungsereignisse beispielsweise enthält vier Monitore, in denen Informationen zu Bedrohungen für das Netzwerk angezeigt werden.

Zum Anzeigen oder Ändern von Dashboards und Monitoren benötigen Sie die entsprechenden Berechtigungen.

Inhalt

- *Verwenden von Dashboards und Monitoren*
- *Verwalten von Dashboards*
- *Exportieren und Importieren von Dashboards*
- *Verwalten von Dashboard-Monitoren*
- *Verschieben und Ändern der Größe von Dashboard-Monitoren*
- *Standard-Dashboards und deren Monitore*
- *Festlegen von ersten Dashboards und Dashboard-Aktualisierungsintervallen*

Verwenden von Dashboards und Monitoren

Sie können die Dashboards und Monitore anpassen, damit Sie die Informationen erhalten, die Sie für Ihre Rolle und Umgebung benötigen.

Die McAfee ePO-Konsole enthält ein Standard-Dashboard, das bei der ersten Anmeldung angezeigt wird. Bei der nächsten Anmeldung wird auf der Seite Dashboards das zuletzt verwendete Dashboard angezeigt.

Wenn Sie alle Standard-Dashboards gelöscht haben, wird beim Starten von McAfee ePO der folgende Text in der Mitte der Dashboard-Seite angezeigt: Es wurden keine Dashboards konfiguriert. Erstellen Sie ein neues Dashboard, oder importieren Sie ein vorhandenes. Informationen zum Erstellen oder Importieren eines Dashboards finden Sie unter *Verwalten von Dashboards* oder *Exportieren und Importieren von Dashboards*.

Sie können zwischen Dashboards wechseln, indem Sie im Dropdown-Menü ein anderes Dashboard auswählen. Sie haben die Wahl zwischen drei verschiedenen Dashboard-Arten.

1 **McAfee-Dashboards**: McAfee-Dashboards sind nicht bearbeitbar und können von allen Benutzern angezeigt werden. Sie können ein McAfee-Dashboard als Ausgangspunkt für eigene angepasste Dashboards duplizieren.

2 **Öffentliche Dashboards**: Öffentliche Dashboards werden von Benutzern erstellt und für andere Benutzer freigegeben.

3 **Private Dashboards**: Diese Dashboards haben Sie für Ihre eigenen Zwecke erstellt. Private Dashboards sind nicht für andere Benutzer freigegeben.

Beim Erstellen eines privaten oder öffentlichen Dashboards können Sie die gewünschten Monitore aus der Monitorgalerie ziehen und im neuen Dashboard ablegen.

Siehe auch

Verwalten von Dashboards auf Seite 260
Verwalten von Dashboard-Monitoren auf Seite 263

Verwalten von Dashboards

Sie können Berechtigungen für Dashboards erstellen, bearbeiten, duplizieren, löschen und diese Berechtigungen zu Dashboards zuweisen.

Bevor Sie beginnen

Zum Ändern eines Dashboards benötigen Sie die entsprechenden Berechtigungen.

Die im Lieferumfang von ePolicy Orchestrator enthaltenen Standard-Dashboards und vordefinierten Abfragen können nicht geändert oder gelöscht werden. Wenn Sie diese Dashboards oder Abfragen ändern möchten, müssen Sie sie duplizieren und umbenennen. Anschließend können Sie das umbenannte Duplikat ändern.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Berichterstellung** | **Dashboards**, um zur Seite **Dashboards** zu gelangen.

2 Wählen Sie eine der folgenden Aktionen aus.

Aktion	Vorgehensweise
Erstellen eines Dashboards	Zum Erstellen einer anderen Ansicht in der Umgebung erstellen Sie ein neues Dashboard. 1 Klicken Sie auf **Dashboard-Aktionen** | **Neu**. 2 Geben Sie einen Namen für das Dashboard ein, wählen Sie eine Option für die Dashboard-Sichtbarkeit aus, und klicken Sie auf **OK**. Ein neues leeres Dashboard wird angezeigt. Dem neuen Dashboard können je nach Bedarf Monitore hinzugefügt werden.
Bearbeiten und Zuweisen von Dashboard-Berechtigungen	Dashboards werden nur Benutzern mit entsprechender Berechtigung angezeigt. Die Dashboards zugewiesenen Berechtigungen sind mit denen von Abfragen oder Berichten identisch. Die Dashboards sind entweder ganz privat, ganz öffentlich oder mit einem oder mehreren Berechtigungssätzen freigegeben. 1 Klicken Sie auf **Dashboard-Aktionen** | **Bearbeiten**. 2 Wählen Sie eine Berechtigung aus: • **Dieses Dashboard nicht freigeben** • **Dieses Dashboard für alle freigeben** • **Dieses Dashboard für die folgenden Berechtigungssätze freigeben** Bei dieser Option müssen Sie außerdem mindestens einen Berechtigungssatz auswählen. 3 Klicken Sie auf **OK**, um das Dashboard zu ändern. Sie können auch ein Dashboard erstellen, das umfangreichere Berechtigungen als eine oder mehrere im Dashboard enthaltene Abfragen besitzt. In solchen Fällen wird Benutzern, die über Zugriff auf die zugrundeliegenden Daten verfügen, beim Öffnen des Dashboards die Abfrage angezeigt. Benutzern ohne Zugriff auf die zugrundeliegenden Daten wird eine Meldung mit dem Inhalt angezeigt, dass sie nicht über die erforderlichen Berechtigungen für diese Abfrage verfügen. Wenn die Abfrage als privat für den Dashboard-Ersteller festgelegt ist, kann sie nur vom Ersteller geändert oder aus dem Dashboard entfernt werden.

Aktion	Vorgehensweise
Duplizieren eines Dashboards	Manchmal lässt sich ein neues Dashboard am einfachsten erstellen, indem ein vorhandenes Dashboard, das dem gewünschten Ergebnis am nächsten kommt, kopiert wird. 1 Klicken Sie auf **Dashboard-Aktionen** | **Duplizieren**. 2 Das Duplikat erhält von ePolicy Orchestrator einen Namen, indem an den Namen des Originals der Hinweis "(Kopie)" angehängt wird. Wenn Sie diesen Namen ändern möchten, geben Sie den gewünschten Namen ein, und klicken Sie auf **OK**. Das duplizierte Dashboard wird nun geöffnet. Das Duplikat ist eine exakte Kopie des Original-Dashboards einschließlich aller Berechtigungen. Nur der Name ist anders.
Löschen eines Dashboards	1 Klicken Sie auf **Dashboard-Aktionen** | **Löschen**. 2 Klicken Sie auf **OK**, um das Dashboard zu löschen. Das Dashboard wurde gelöscht, und es wird das Standard-Dashboard des Systems angezeigt. Benutzern, denen das gelöschte Dashboard vor dem Abmelden als letztes Dashboard angezeigt wurde, wird bei ihrer nächsten Anmeldung das Standard-Dashboard des Systems angezeigt.

Siehe auch

Verwenden von Dashboards und Monitoren auf Seite 259

Exportieren und Importieren von Dashboards

Nachdem Sie Ihre Dashboards und Monitore fertig definiert haben, können diese am schnellsten auf andere McAfee ePO-Server migriert werden, indem Sie sie exportieren und auf den anderen Servern importieren.

Bevor Sie beginnen

Für den Import eines Dashboards müssen Sie Zugriff auf ein zuvor exportiertes, in einer XML-Datei enthaltenes Dashboard haben.

Ein als XML-Datei exportiertes Dashboard kann in dasselbe oder ein anderes System importiert werden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Berichterstellung** | **Dashboards**.

2 Wählen Sie eine der folgenden Aktionen aus.

Aktion	Vorgehensweise
Exportieren von Dashboards	1 Klicken Sie auf **Dashboard-Aktionen** | **Exportieren**. Ihr Browser versucht, gemäß den Browser-Einstellungen eine XML-Datei herunterzuladen. 2 Speichern Sie die exportierte XML-Datei in einem geeigneten Speicherort.
Importieren von Dashboards	1 Klicken Sie auf **Dashboard-Aktionen** | **Importieren**. Das Dialogfeld Dashboard importieren wird angezeigt. 2 Klicken Sie auf **Durchsuchen**, und wählen Sie die XML-Datei aus, die ein exportiertes Dashboard enthält. Klicken Sie auf **Öffnen**. 3 Klicken Sie auf **Speichern**. Das Bestätigungsdialogfeld Dashboard importieren wird angezeigt. Der Name des Dashboards in der Datei sowie der Name, den es im System haben wird, werden angezeigt. Standardmäßig ist dies der Name, unter dem das Dashboard exportiert wurde, an den der Zusatz "(importiert)" angehängt ist. 4 Klicken Sie auf **OK**. Wenn Sie das Dashboard nicht importieren möchten, klicken Sie auf **Schließen**. Das importierte Dashboard wird angezeigt. Unabhängig von den Berechtigungen zum Zeitpunkt des Exports werden importierten Dashboards eigene Berechtigungen zugewiesen. Nach dem Import müssen Sie die Berechtigungen explizit festlegen.

Verwalten von Dashboard-Monitoren

Sie können Monitore für Dashboards erstellen, zu Dashboards hinzufügen und aus diesen entfernen.

Bevor Sie beginnen

Sie benötigen Schreibberechtigungen für das Dashboard, das Sie ändern möchten.

Wenn Sie nicht über die notwendigen Rechte oder Produktlizenzen zum Anzeigen eines Monitors verfügen oder die zugrunde liegende Abfrage für den Monitor nicht mehr verfügbar ist, wird anstelle des Monitors eine entsprechende Meldung angezeigt.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Berichterstellung** | **Dashboards**. Wählen Sie in der Dropdown-Liste **Dashboard** ein Dashboard aus.

2 Wählen Sie eine der folgenden Aktionen aus.

Aktion	Vorgehensweise
Hinzufügen eines Monitors	**1** Klicken Sie auf **Monitor hinzufügen**. Die **Monitorgalerie** wird oben auf dem Bildschirm angezeigt. **2** Wählen Sie in der Dropdown-Liste **Anzeigen** eine Monitorkategorie aus. Die in dieser Kategorie verfügbaren Monitore werden in der Galerie angezeigt. **3** Ziehen Sie einen Monitor auf das Dashboard. Wenn Sie den Cursor im Dashboard bewegen, wird die jeweils nächstgelegene verfügbare Position hervorgehoben, an der der Monitor abgelegt werden kann. Legen Sie den Monitor an der gewünschten Position ab. Das Dialogfeld **Neuer Monitor** wird angezeigt. **4** Konfigurieren Sie den Monitor gemäß Ihren Anforderungen (jeder Monitor hat seine eigenen Konfigurationsoptionen), und klicken Sie dann auf **OK**. **5** Wenn Sie die Monitore zum Dashboard hinzugefügt haben, klicken Sie auf **Speichern**, um das neu konfigurierte Dashboard zu speichern. **6** Klicken Sie nach Abschluss Ihrer Änderungen auf **Schließen**. Wenn Sie zu einem Dashboard einen Monitor vom Typ **Anzeige für benutzerdefinierte URLs** hinzufügen, der Adobe Flash-Inhalte oder ActiveX-Steuerelemente enthält, werden durch diese Inhalte möglicherweise Menüs von ePolicy Orchestrator verdeckt, sodass auf Teile des Menüs nicht mehr zugegriffen werden kann.
Bearbeiten eines Monitors	Von jedem Monitortyp werden andere Konfigurationsoptionen unterstützt. Bei einem Abfragemonitor wären das zum Beispiel Änderungen an der Abfrage, der Datenbank und dem Aktualisierungsintervall. **1** Wählen Sie einen Monitor aus, den Sie verwalten möchten, klicken Sie auf den Pfeil in seiner oberen linken Ecke, und wählen Sie **Monitor bearbeiten** aus. Das Dialogfeld für die Konfiguration des Monitors wird angezeigt. **2** Wenn Sie die gewünschten Änderungen an den Einstellungen des Monitors vorgenommen haben, klicken Sie auf **OK**. Wenn Sie keine Änderungen vornehmen möchten, klicken Sie auf **Abbrechen**. **3** Wenn Sie die damit verbundenen Änderungen am Dashboard speichern möchten, klicken Sie auf **Speichern**. Andernfalls klicken Sie auf **Verwerfen**.
Entfernen eines Monitors	**1** Wählen Sie einen Monitor aus, den Sie entfernen möchten, klicken Sie auf den Pfeil in seiner oberen linken Ecke, und wählen Sie **Monitor entfernen** aus. Das Dialogfeld für die Konfiguration des Monitors wird angezeigt. **2** Wenn Sie die Änderungen am Dashboard vorgenommen haben, klicken Sie auf **Speichern**. Klicken Sie auf **Verwerfen**, wenn Sie das Dashboard auf seine vorherigen Einstellungen zurücksetzen möchten.

Siehe auch

Verwenden von Dashboards und Monitoren auf Seite 259

Verschieben und Ändern der Größe von Dashboard-Monitoren

Monitore können so verschoben und in der Größe angepasst werden, dass der Platz auf dem Bildschirm effizient genutzt wird.

> **Bevor Sie beginnen**
> Sie benötigen Schreibberechtigungen für das Dashboard, das Sie ändern möchten.

Sie können bei vielen Dashboard-Monitoren die Größe ändern. Wenn rechts unten im Monitor kleine diagonale Linien angezeigt werden, können Sie dessen Größe ändern. Monitore werden mittels Ziehen und Ablegen innerhalb des aktuellen Dashboards verschoben und in der Größe verändert.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Verschieben Sie einen Monitor, oder ändern Sie dessen Größe.

- So verschieben Sie einen Dashboard-Monitor
  1 Ziehen Sie den Monitor an seiner Titelleiste an die gewünschte Position.

    Wenn Sie den Cursor bewegen, wird der Umriss des Monitors an die nächste für ihn verfügbare Position verschoben.

  2 Wenn sich der Umriss an der gewünschten Position befindet, legen Sie den Monitor dort ab.

    Wenn Sie versuchen, den Monitor an einer unzulässigen Stelle abzulegen, kehrt er an seine vorherige Position zurück.

- So ändern Sie die Größe eines Dashboard-Monitors
  1 Ziehen Sie das Symbol für die Größenänderung in der rechten unteren Ecke des Monitors zu einer geeigneten Position.

    Während Sie den Cursor bewegen, ändert der Umriss des Monitors seine Form und zeigt die in der jeweiligen Cursor-Position unterstützte Größe an. Für Monitore kann es Beschränkungen hinsichtlich der minimalen oder maximalen Größe geben.

  2 Wenn der Umriss die gewünschte Größe aufweist, lassen Sie die Maustaste los.

    Wenn Sie den Monitor auf eine Größe einstellen möchten, die an der derzeitigen Position des Monitors nicht möglich ist, wird die vorherige Größe wiederhergestellt.

2 Klicken Sie auf **Speichern**. Wenn Sie die vorherige Konfiguration wiederherstellen möchten, klicken Sie auf **Verwerfen**.

Standard-Dashboards und deren Monitore

ePolicy Orchestrator enthält verschiedene Standard-Dashboards, die jeweils eigene Standardmonitore enthalten.

Alle Dashboards außer dem Standard-Dashboard (meist McAfee ePO-Übersicht) werden von dem Administrator verwaltet, der McAfee ePO installiert hat. Der Administrator, der die Installation durchgeführt hat, muss die Berechtigungen für zusätzliche Dashboards ändern, damit andere McAfee ePO-Benutzer sie anzeigen können.

Entsprechend sind möglicherweise auch zum Anzeigen einiger Monitore innerhalb eines Dashboards weitere Berechtigungen erforderlich.

Dashboard Audit

Im Dashboard **Audit** erhalten Sie einen Überblick über Aktivitäten auf einem McAfee ePO-Server, die mit Zugriffen in Verbindung stehen. Dieses Dashboard enthält die folgenden Monitore:

- **Fehlgeschlagene Anmeldeversuche in den letzten 30 Tagen** – Zeigt eine nach Benutzer gruppierte Liste aller fehlgeschlagenen Anmeldeversuche in den letzten 30 Tagen an.
- **Erfolgreiche Anmeldeversuche in den letzten 30 Tagen** – Zeigt eine nach Benutzer gruppierte Liste aller erfolgreichen Anmeldeversuche in den letzten 30 Tagen an.
- **Änderungsverlauf von Richtlinienzuweisungen nach Benutzer**: Zeigt einen nach Benutzer gruppierten Bericht an, der alle Richtlinienzuweisungen aus den letzten 30 Tagen aus dem Audit-Protokoll enthält.
- **Konfigurationsänderungen nach Benutzer**: Zeigt einen nach Benutzer gruppierten Bericht an, der alle als sensibel geltenden Aktionen der letzten 30 Tage aus dem Audit-Protokoll enthält.
- **Server-Konfigurationen nach Benutzer**: Zeigt einen nach Benutzer gruppierten Bericht an, der alle Server-Konfigurationsaktionen der letzten 30 Tage aus dem Audit-Protokoll enthält.
- **Schnelle Systemsuche** – Sie können nach Systemen anhand des Systemnamens, der IP-Adresse, der MAC-Adresse, dem Benutzernamen oder der Agenten-GUID suchen.

Dashboard McAfee ePO-Zusammenfassung

Das Dashboard McAfee ePO-Übersicht besteht aus Monitoren, die zusammengefasste Informationen und Links zu weiteren Informationen von McAfee enthalten. Dieses Dashboard enthält die folgenden Monitore:

- **Systeme pro Gruppe der obersten Ebene**: Zeigt ein Balkendiagramm der verwalteten Systeme an, organisiert nach der obersten Systemstrukturgruppe.
- **Schnelle Systemsuche** – Sie können nach Systemen anhand des Systemnamens, der IP-Adresse, der MAC-Adresse, dem Benutzernamen oder der Agenten-GUID suchen.
- **McAfee-Links**: Zeigt unter anderem Links zum technischen Support von McAfee, zu Eskalations-Tools und zur Virusinformationsbibliothek an.
- **Compliance-Übersicht von McAfee Agent und VirusScan Enterprise (für Windows)**: Zeigt in einem booleschen Kreisdiagramm an, welche verwalteten Systeme in der Umgebung mit der Version von VirusScan Enterprise (für Windows), McAfee Agent und den DAT-Dateien konform bzw. nicht konform sind.
- **Malware-Entdeckungsverlauf** – Zeigt ein Liniendiagramm mit der Anzahl der internen Virenentdeckungen innerhalb des letzten Quartals an.

Management-Dashboard

Das Management-Dashboard besteht aus Monitoren mit zusammengefassten Berichten zu Sicherheitsbedrohungen und Links zu spezielleren Produktinformationen von McAfee. Dieses Dashboard enthält die folgenden Monitore:

- **Malware-Entdeckungsverlauf** – Zeigt ein Liniendiagramm mit der Anzahl der internen Virenentdeckungen innerhalb des letzten Quartals an.
- **Produktausbringungen in den letzten 24 Stunden** – Zeigt ein boolesches Kreisdiagramm aller Produktausbringungen der letzten 24 Stunden an. Erfolgreiche Ausbringungen werden grün dargestellt.
- **Produktaktualisierungen in den letzten 24 Stunden** – Zeigt ein boolesches Kreisdiagramm aller Produktaktualisierungen der letzten 24 Stunden an. Erfolgreiche Aktualisierungen werden grün dargestellt.

Dashboard Erste Schritte mit ePolicy Orchestrator

Das Dashboard Erste Schritte mit ePolicy Orchestrator besteht aus Monitoren, in denen Sie sich über McAfee ePO informieren und die Installations-URL für die Produkt-Software erstellen können. Standardmäßig ist das Dashboard Erste Schritte mit ePolicy Orchestrator das erste, das Benutzern angezeigt wird, wenn sie sich erstmals bei McAfee ePO anmelden. Dieses Dashboard enthält die folgenden Monitore:

- **Willkommen bei ePolicy Orchestrator**: Zeigt eine Präsentation an, in der Sie sich mit der Software und ihrer Funktionsweise vertraut machen können.
- **Erste Schritte**: Zeigt die Liste der Produkte an, die Sie auf den verwalteten Computern installieren können.

Dashboard Produktbereitstellung

Im Dashboard **Produktausbringung** erhalten Sie einen Überblick über Aktivitäten im Netzwerk bezüglich der Ausbringung und Aktualisierung von Produkten. Dieses Dashboard verfügt über die folgenden Monitore:

- **Produktausbringungen in den letzten 24 Stunden** – Zeigt ein boolesches Kreisdiagramm aller Produktausbringungen der letzten 24 Stunden an. Erfolgreiche Ausbringungen werden grün dargestellt.
- **Produktaktualisierungen in den letzten 24 Stunden** – Zeigt ein boolesches Kreisdiagramm aller Produktaktualisierungen der letzten 24 Stunden an. Erfolgreiche Aktualisierungen werden grün dargestellt.
- **Fehlgeschlagene Produktausbringungen in den letzten 24 Stunden**: Zeigt ein nach Produkt-Codes gruppiertes Diagramm mit einem Balken an, das alle in den letzten 24 Stunden fehlgeschlagenen Produktausbringungen enthält.
- **Schnelle Systemsuche** – Sie können nach Systemen anhand des Systemnamens, der IP-Adresse, der MAC-Adresse, dem Benutzernamen oder der Agenten-GUID suchen.
- **Fehlgeschlagene Produktaktualisierungen in den letzten 24 Stunden** – Zeigt ein nach Produkt-Codes gruppiertes Diagramm mit einem Balken an, das alle in den letzten 24 Stunden fehlgeschlagenen Produktaktualisierungen enthält.
- **Versuchte Agenten-Deinstallationen in den letzten 7 Tagen** – Zeigt ein nach Tagen gruppiertes Diagramm mit einem Balken an, das alle Agenten-Deinstallationsereignisse auf Clients aus den letzten 7 Tagen enthält.

Festlegen von ersten Dashboards und Dashboard-Aktualisierungsintervallen

Mit der Server-Einstellung Dashboards wird das Dashboard, das einem Benutzer nach dem ersten Anmelden angezeigt wird, sowie die Aktualisierungshäufigkeit für alle Dashboards angegeben.

Sie können festlegen, welches Dashboard einem Benutzer nach dem erstmaligen Anmelden angezeigt werden soll, indem Sie dieses Dashboard dem Berechtigungssatz des Benutzers zuordnen. Durch das Zuordnen von Dashboards zu Berechtigungssätzen wird sichergestellt, dass Benutzern, denen eine bestimmte Rolle zugewiesen wurde, automatisch die benötigten Informationen angezeigt werden. Benutzern, die neben ihrem Standard-Dashboard auch andere Dashboards anzeigen dürfen, wird beim Wechseln auf die Seite **Dashboards** das zuletzt geöffnete Dashboard angezeigt.

Mithilfe der Server-Einstellung Dashboards können Sie folgende Aktionen durchführen:

- Sie können konfigurieren, welches Dashboard einem Benutzer angezeigt wird, der zu einem Berechtigungssatz gehört, der keine Standard-Dashboard-Zuweisung besitzt.
- Sie können die automatische Aktualisierungsrate für Dashboards steuern.

Dashboards werden automatisch aktualisiert. Bei jedem Aktualisierungsvorgang wird die zugrunde liegende Abfrage ausgeführt, und die Ergebnisse werden im Dashboard angezeigt. Bei Abfrageergebnissen, die große Datenmengen enthalten, kann sich ein kurzes Aktualisierungsintervall negativ auf die verfügbare Bandbreite auswirken. Sie sollten daher ein Aktualisierungsintervall wählen, das kurz genug ist, dass korrekte und aktuelle Informationen angezeigt werden, ohne dass Netzwerkressourcen übermäßig in Anspruch genommen werden. Das Standardintervall beträgt fünf Minuten.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste **Einstellungskategorien** den Eintrag **Dashboards** aus, und klicken Sie dann auf **Bearbeiten**.

2 Wählen Sie in den Menüs einen Berechtigungssatz und ein Standard-Dashboard aus.

Mithilfe der Schaltfläche und können Sie bei jedem Berechtigungssatz oder bei Zuweisungen für mehrere Berechtigungssätze mehrere Dashboards hinzufügen oder entfernen.

3 Geben Sie für das Dashboard-Monitor-Aktualisierungsintervall (das standardmäßig 5 Minuten beträgt) einen Wert zwischen 1 Minute und 60 Stunden an, und klicken Sie dann auf **Speichern**.

21 Abfragen und Berichte

ePolicy Orchestrator verfügt über eigene Funktionen für Abfragen und Berichterstellung. Enthalten sind der Abfrage-Generator und der Bericht-Generator, mit denen Sie Abfragen und Berichte erstellen und ausführen können, die benutzerkonfigurierte Daten in benutzerkonfigurierten Diagrammen und Tabellen ausgeben. Die Daten für diese Abfragen und Berichte können aus beliebigen registrierten internen oder externen Datenbanken im ePolicy Orchestrator-System stammen.

Zusätzlich zum Abfrage- und Berichterstellungssystem können Sie mithilfe der folgenden Protokolle Informationen zu Aktivitäten erfassen, die auf dem McAfee ePO-Server und im Netzwerk stattfinden:

- Audit-Protokoll
- Server-Task-Protokoll
- Bedrohungsereignisprotokoll

Inhalt

- *Berechtigungen für Abfragen und Berichte*
- *Informationen zu Abfragen*
- *Abfragen-Generator*
- *Erstmaliges Konfigurieren von Abfragen und Berichten*
- *Arbeiten mit Abfragen*
- *Zusammengefasste Abfragen mehrerer Server*
- *Informationen zu Berichten*
- *Struktur von Berichten*
- *Arbeiten mit Berichten*

Berechtigungen für Abfragen und Berichte

Es gibt eine Reihe von Möglichkeiten, den Zugriff auf Abfragen und Berichte zu beschränken. Um eine Abfrage oder einen Bericht auszuführen, benötigen Sie nicht nur für diese Abfrage oder diesen Bericht Berechtigungen, sondern auch für die Funktionssätze, die mit den jeweiligen Ergebnistypen verbundenen sind. Die Ergebnisseiten einer Abfrage bieten nur Zugriff auf Aktionen, die entsprechend Ihren Berechtigungssätzen zugelassen sind.

Gruppen und Berechtigungssätze steuern den Zugriff auf Abfragen und Berichte. Alle Abfragen und Berichte müssen zu einer Gruppe gehören, und der Zugriff auf diese Abfrage bzw. diesen Bericht wird von der Berechtigungsebene der Gruppe gesteuert. Abfrage- und Berichtgruppen können eine der folgenden Berechtigungsebenen haben:

- **Privat** – Die Gruppe ist nur für den Benutzer verfügbar, der sie erstellt hat.
- **Öffentlich** – Die Gruppe ist global freigegeben.
- **Nach Berechtigungssatz** – Die Gruppe ist nur für Benutzer verfügbar, denen die ausgewählten Berechtigungssätze zugewiesen wurden.

Berechtigungssätze verfügen über vier Zugriffsebenen für Abfragen oder Berichte. Zu diesen Berechtigungen gehören:

- **Keine Berechtigungen** – Benutzern ohne Berechtigungen wird die Registerkarte **Abfrage** oder **Bericht** nicht angezeigt.
- **Öffentliche Abfragen verwenden** – Gewährt die Berechtigung zum Verwenden aller Abfragen oder Berichte, die in eine **Öffentliche Gruppe** abgelegt wurden.
- **Öffentliche Abfragen verwenden; persönliche Abfragen erstellen und bearbeiten** – Gewährt die Berechtigung zum Verwenden aller Abfragen oder Berichte, die in eine **Öffentliche Gruppe** abgelegt wurden. Außerdem können mit dem **Abfragen-Generator** Abfragen oder Berichte in **Privaten Gruppen** erstellt und bearbeitet werden.
- **Öffentliche Abfragen bearbeiten; persönliche Abfragen erstellen und bearbeiten; persönliche Abfragen veröffentlichen** – Gewährt die Berechtigung zum Verwenden und Bearbeiten aller Abfragen oder Berichte, die in **Öffentlichen Gruppen** abgelegt wurden, sowie zum Erstellen und Bearbeiten von Abfragen oder Berichten in **Privaten Gruppen**. Außerdem können Abfragen oder Berichte von **Privaten Gruppen** in **Öffentliche Gruppen** oder **Freigegebene Gruppen** verschoben werden.

Informationen zu Abfragen

Abfragen sind im Wesentlichen Fragen, die Sie an ePolicy Orchestrator stellen, und die Antworten werden in verschiedenen Diagramm- und Tabellenformen zurückgegeben.

Eine Abfrage kann einzeln verwendet werden, um sofort eine Antwort zu erhalten. Alle Abfrageergebnisse können in verschiedenen Formaten exportiert werden, die jeweils heruntergeladen oder als Anhang einer E-Mail-Nachricht gesendet werden können. Die meisten Abfragen können auch als Dashboard-Monitore verwendet werden und ermöglichen dann eine Systemüberwachung in nahezu Echtzeit. Zudem können Abfragen in Berichte aufgenommen werden und ermöglichen dann eine umfassendere und systematischere Betrachtung Ihres ePolicy Orchestrator-Systems.

Die im Lieferumfang von ePolicy Orchestrator enthaltenen Standard-Dashboards und vordefinierten Abfragen können nicht geändert oder gelöscht werden. Wenn Sie diese Dashboards oder Abfragen ändern möchten, müssen Sie sie duplizieren und umbenennen. Anschließend können Sie das umbenannte Duplikat ändern.

An Abfrageergebnissen lassen sich Aktionen durchführen

Für Abfrageergebnisse können Aktionen ausgeführt werden. Für die in Tabellen (und Drilldown-Tabellen) angezeigten Abfrageergebnisse ist bei ausgewählten Elementen in der Tabelle eine Reihe von Aktionen verfügbar. So können Sie beispielsweise Agenten auf Systemen bereitstellen, die in einer Tabelle mit Abfrageergebnissen aufgelistet sind. Aktionen stehen unten auf der Ergebnisseite zur Verfügung.

Abfragen als Dashboard-Monitore

Die meisten Abfragen (außer solchen, bei denen die ursprünglichen Ergebnisse mithilfe einer Tabelle angezeigt werden) eignen sich als Dashboard-Monitor. Dashboard-Monitore werden innerhalb benutzerdefinierter Intervalle (Standard sind fünf Minuten) automatisch aktualisiert.

Exportierte Ergebnisse

Abfrageergebnisse lassen sich in vier verschiedenen Formaten exportieren. Bei exportierten Ergebnissen handelt es sich um Verlaufsdaten. Sie werden im Gegensatz zu anderen Monitoren, die als Dashboard-Monitore verwendet werden, nicht aktualisiert. Wie bei den in der Konsole angezeigten Abfrageergebnissen und abfragebasierten Monitoren können Sie HTML-Exporte nach detaillierteren Informationen aufgliedern.

Im Gegensatz zu Abfrageergebnissen in der Konsole sind Daten in exportierten Berichten nicht für Aktionen geeignet.

Berichte sind in den folgenden Formaten verfügbar:

- CSV – Verwenden Sie dieses Format, um die Daten in einer Tabellenkalkulationsanwendung (z. B. Microsoft Excel) zu verwenden.
- XML – Verwenden Sie dieses Format, um die Daten für andere Zwecke zu transformieren.
- HTML – Verwenden Sie dieses Format, um die exportierten Ergebnisse als Webseite anzuzeigen.
- PDF – Verwenden Sie dieses Format, wenn Sie die Ergebnisse ausdrucken möchten.

Einbinden von Abfragen in Berichte

Berichte können beliebig viele Abfragen, Bilder, statische Texte und andere Elemente enthalten. Sie können bei Bedarf oder nach einem regelmäßigen Zeitplan ausgeführt werden und werden zum Anzeigen außerhalb von ePolicy Orchestrator als PDF-Datei ausgegeben.

Freigeben von Abfragen zwischen Servern

Jede Abfrage kann importiert und exportiert werden. Hierdurch können Sie Abfragen zwischen Servern freigeben. Dadurch müssen Abfragen in Umgebungen mit mehreren Servern nur einmal erstellt werden.

Abrufen von Daten aus unterschiedlichen Quellen

Mit Abfragen können Daten von jedem registrierten Server abgerufen werden, auch von ePolicy Orchestrator-externen Datenbanken.

Abfragen-Generator

ePolicy Orchestrator enthält einen einfachen Assistenten, mit dem Sie benutzerdefinierte Abfragen in vier Schritten erstellen und bearbeiten können. Mit dem Assistenten können Sie konfigurieren, welche Daten abgerufen und angezeigt werden. Darüber hinaus können Sie angeben, in welcher Form sie angezeigt werden.

Ergebnistypen

Als erstes wählen Sie im Abfragen-Generator das Schema und den Ergebnistyp aus einer Funktionsgruppe aus. Damit geben Sie an, woher die Abfrage Daten abruft, welcher Typ von Daten abgerufen wird und welche weiteren Auswahlmöglichkeiten auf den restlichen Seiten des Assistenten zur Verfügung stehen.

Diagrammtypen

ePolicy Orchestrator verfügt über eine Reihe von Diagrammen und Tabellen zum Anzeigen der abgerufenen Daten. Diese Diagramme und Tabellen und deren Aufgliederungstabellen sind in hohem Maße konfigurierbar.

Aufgliederungstabellen gehören nicht zu den Tabellen.

Zu den Diagrammtypen gehören:

Tabelle 21-1 Diagrammtypgruppen

Typ	Diagramm oder Tabelle
Balken	• Balkendiagramm • Diagramm mit gruppierten Balken • Gestapeltes Balkendiagramm
Kreis	• Boolesches Kreisdiagramm • Kreisdiagramm
Blase	• Blasendiagramm
Zusammenfassung	• Gruppierte Übersichtstabelle mit mehreren Gruppen • Gruppierte Übersichtstabelle mit einer Gruppe
Linie	• Diagramm mit mehreren Linien • Diagramm mit einer Linie
Liste	• Tabelle

Tabellenspalten

Geben Sie Spalten für die Tabelle an. Wenn Sie **Tabelle** als primäre Ansicht der Daten auswählen, wird diese Tabelle konfiguriert. Wenn Sie als erste Ansicht der Daten einen Diagrammtyp auswählen, wird die Aufgliederungstabelle konfiguriert.

An den in einer Tabelle angezeigten Abfrageergebnisse lassen sich Aktionen durchführen. Wenn die Tabelle beispielsweise mit Systemen aufgefüllt ist, können Sie Agenten für diese Systeme direkt aus der Tabelle ausbringen oder reaktivieren.

Filter

Legen Sie durch Auswählen von Eigenschaften und Operatoren spezielle Kriterien fest, um die von der Abfrage abgerufenen Daten einzuschränken.

Erstmaliges Konfigurieren von Abfragen und Berichten

Gehen Sie wie nachfolgend allgemein beschrieben vor, wenn Sie zum ersten Mal Abfragen und Berichte konfigurieren.

1 Machen Sie sich mit den Funktionen von Abfragen, Berichten und dem Abfragen-Generator vertraut.

2 Sehen Sie sich die Standardabfragen und -berichte an, und bearbeiten Sie sie nach Bedarf.

3 Erstellen Sie Abfragen und Berichte für alle Anforderungen, die durch die Standardabfragen nicht abgedeckt werden.

Arbeiten mit Abfragen

Abfragen können je nach Ihren Anforderungen u. a. ausgeführt und exportiert werden.

Aufgaben

- *Verwalten benutzerdefinierter Abfragen* auf Seite 273
  Sie können Abfragen nach Bedarf erstellen, duplizieren, bearbeiten und löschen.
- *Ausführen einer Abfrage* auf Seite 275
  Sie können gespeicherte Abfragen bei Bedarf ausführen.
- *Planmäßiges Ausführen einer Abfrage* auf Seite 275
  Zum regelmäßigen Ausführen einer Abfrage wird ein Server-Task verwendet. Abfragen können Unteraktionen umfassen, mit denen Sie eine Reihe von Tasks ausführen können. Darunter fallen das Senden von Abfrageergebnissen per E-Mail und der Einsatz von Tags.
- *Erstellen einer Abfragegruppe* auf Seite 276
  Mithilfe von Abfragegruppen können Sie Abfragen oder Berichte speichern, ohne anderen Benutzern den Zugriff darauf zu erlauben.
- *Verschieben einer Abfrage in eine andere Gruppe* auf Seite 277
  Ändern die Berechtigungen für eine Abfrage, indem Sie die Abfrage in eine andere Gruppe verschieben.
- *Exportieren und Importieren von Abfragen* auf Seite 277
  Netzwerkinformationen sind sehr detailliert. Durch Exportieren und Importieren von einem Server auf einen anderen kann sichergestellt werden, dass der Datenabruf auf allen McAfee ePO-Servern konsistent erfolgt.
- *Exportieren von Abfrageergebnissen in andere Formate* auf Seite 278
  Abfrageergebnisse können in die folgenden Formate exportiert werden: HTML, PDF, CSV und XML.

Verwalten benutzerdefinierter Abfragen

Sie können Abfragen nach Bedarf erstellen, duplizieren, bearbeiten und löschen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Öffnen Sie die Seite Abfragen und Berichte: Klicken Sie auf **Menü** | **Berichterstellung** | **Abfragen und Berichte**.

2 Wählen Sie eine der folgenden Aktionen aus:

Aktion	Vorgehensweise
Erstellen von benutzerdefinierten Abfragen	1 Klicken Sie auf **Neue Abfrage**. Daraufhin wird der Abfrage-Generator angezeigt. 2 Wählen Sie auf der Seite Ergebnistyp die **Funktionsgruppe** und den **Ergebnistyp** für diese Abfrage aus, und klicken Sie dann auf **Weiter**. 3 Wählen Sie den Typ von Diagramm oder Tabelle aus, mit dem die primären Ergebnisse der Abfrage dargestellt werden sollen, und klicken Sie dann auf **Weiter**. Wenn Sie **Boolesches Kreisdiagramm** auswählen, müssen Sie noch die Kriterien konfigurieren, die in der Abfrage enthalten sein sollen. 4 Wählen Sie die Spalten aus, die in der Abfrage enthalten sein sollen, und klicken Sie dann auf **Weiter**. Wenn Sie auf der Seite **Diagramm** die Option Tabelle ausgewählt haben, besteht die Tabelle aus den hier ausgewählten Spalten. Andernfalls bilden diese Spalten die Tabelle mit den Abfragedetails. 5 Wählen Sie Eigenschaften aus, um die Suchergebnisse einzugrenzen, und klicken Sie dann auf **Ausführen**. Auf der Seite Nicht gespeicherte Abfrage werden die Ergebnisse der Abfrage angezeigt, für die Aktionen durchgeführt werden können. Sie können daher alle verfügbaren Aktionen für Elemente in sämtlichen Tabellen oder Drilldown-Tabellen durchführen. Ausgewählte Eigenschaften werden im Inhaltsbereich mit Operatoren angezeigt. Mit diesen können Sie Kriterien festlegen, nach denen die für die jeweilige Eigenschaft zurückgegebenen Daten eingegrenzt werden. • Wenn für die Abfrage nicht die erwarteten Ergebnisse zurückgegeben wurden, klicken Sie auf **Abfrage bearbeiten**, um zum **Abfrage-Generator** zurückzukehren und die Details der Abfrage zu bearbeiten. • Wenn Sie die Abfrage nicht speichern möchten, klicken Sie auf **Schließen**. • Wenn Sie diese Abfrage zu einem späteren Zeitpunkt erneut verwenden möchten, klicken Sie auf **Speichern**, und fahren Sie dann mit dem nächsten Schritt fort. 6 Die Seite Abfrage speichern wird angezeigt. Geben Sie einen Namen für die Abfrage ein, fügen Sie Anmerkungen hinzu, und wählen Sie eine der folgenden Optionen aus: • **Neue Gruppe** – Geben Sie den Namen der neuen Gruppe ein, und wählen Sie eine der folgenden Optionen: • **Private Gruppe (Eigene Gruppen)** • **Öffentliche Gruppe (Freigegebene Gruppen)** • **Vorhandene Gruppe** – Wählen Sie die Gruppe in der Liste **Freigegebene Gruppen** aus. 7 Klicken Sie auf **Speichern**. Die neue Abfrage wird in der Liste Abfragen angezeigt.
Duplizieren einer Abfrage	1 Wählen Sie in der Liste die zu kopierende Abfrage aus, und klicken Sie dann auf **Aktionen** | **Duplizieren**.

Aktion	Vorgehensweise
	2 Geben Sie im Dialogfeld **Duplizieren** einen Namen für das Duplikat ein, und wählen Sie eine Gruppe aus, die eine Kopie der Abfrage erhalten soll. Klicken Sie anschließend auf **OK**. Die duplizierte Abfrage wird in der Liste Abfragen angezeigt.
Bearbeiten einer Abfrage	1 Wählen Sie in der Liste die zu bearbeitende Abfrage aus, und klicken Sie dann auf **Aktionen** | **Bearbeiten**. 2 Bearbeiten Sie die Einstellungen der Abfrage, und klicken Sie dann auf **Speichern**. Die geänderte Abfrage wird in der Liste Abfragen angezeigt.
Löschen einer Abfrage	1 Wählen Sie in der Liste die zu löschende Abfrage aus, und klicken Sie dann auf **Aktionen** | **Löschen**. 2 Klicken Sie im angezeigten Bestätigungsdialogfeld auf **Ja**. Die Abfrage wird nicht mehr in der Liste Abfragen angezeigt. Berichte oder Server-Tasks, in denen die gelöschte Abfrage verwendet wurde, werden so lange als ungültig angezeigt, bis in ihnen der Verweis auf die gelöschte Abfrage entfernt wird.

Ausführen einer Abfrage

Sie können gespeicherte Abfragen bei Bedarf ausführen.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Berichterstellung** | **Abfragen und Berichte**, und wählen Sie dann eine Abfrage in der Liste **Abfragen** aus.

2 Klicken Sie auf **Aktionen** | **Ausführen**. Die Ergebnisse der Abfrage werden angezeigt. Sie können den Bericht weiter aufgliedern und nach Bedarf Aktionen an Elementen durchführen.

Welche Aktionen verfügbar sind, hängt von den Berechtigungen des Benutzers ab.

3 Klicken Sie auf **Schließen**, wenn Sie alle gewünschten Vorgänge durchgeführt haben.

Planmäßiges Ausführen einer Abfrage

Zum regelmäßigen Ausführen einer Abfrage wird ein Server-Task verwendet. Abfragen können Unteraktionen umfassen, mit denen Sie eine Reihe von Tasks ausführen können. Darunter fallen das Senden von Abfrageergebnissen per E-Mail und der Einsatz von Tags.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Öffnen Sie den Generator für Server-Tasks.

a Wählen Sie auf der Seite Abfragen und Berichte eine Abfrage aus.

b Wählen Sie die folgenden Optionen aus: **Aktionen** | **Plan**.

2 Geben Sie auf der Seite Beschreibung einen Namen und eine Beschreibung für den Task ein, und klicken Sie dann auf **Weiter**.

3 Wählen Sie im Dropdown-Menü **Aktionen** den Eintrag **Abfrage ausführen** aus.

4 Suchen Sie im Feld **Abfrage** die Abfrage, die Sie ausführen möchten.

5 Wählen Sie die Sprache aus, in der die Ergebnisse angezeigt werden sollen.

6 Wählen Sie in der Liste **Unteraktionen** eine Aktion aus, die basierend auf den Ergebnissen ausgeführt werden soll. Welche Unteraktionen verfügbar sind, hängt von den Berechtigungen des Benutzers und den Produkten ab, die über den McAfee ePO-Server verwaltet werden.

Sie können auch mehrere Aktionen für die Abfrageergebnisse auswählen. Klicken Sie auf die Schaltfläche **+**, um Aktionen hinzuzufügen, die für die Abfrageergebnisse ausgeführt werden sollen. Achten Sie dabei darauf, die Aktionen in der Reihenfolge anzuordnen, in der sie für die Abfrageergebnisse ausgeführt werden sollen.

7 Klicken Sie auf **Weiter**.

8 Planen Sie den Task, und klicken Sie dann auf **Weiter**.

9 Überprüfen Sie die Konfiguration des Tasks, und klicken Sie dann auf **Speichern**.

Der Task wird zur Liste auf der Seite Server-Tasks hinzugefügt. Wenn der Task aktiviert ist (Standardeinstellung), wird er zum nächsten geplanten Zeitpunkt ausgeführt. Ein deaktivierter Task wird nur dann ausgeführt, wenn Sie auf der Seite **Server-Tasks** neben dem Task auf Ausführen klicken.

Erstellen einer Abfragegruppe

Mithilfe von Abfragegruppen können Sie Abfragen oder Berichte speichern, ohne anderen Benutzern den Zugriff darauf zu erlauben.

Durch Erstellen einer Gruppe können Sie Abfragen und Berichte nach ihrer Funktion kategorisieren und den Zugriff auf diese Elemente steuern. Die in ePolicy Orchestrator angezeigte Liste von Gruppen enthält sowohl die von Ihnen erstellten Gruppen als auch die, für die Sie Anzeigeberechtigungen besitzen.

Beim Speichern einer benutzerdefinierten Abfrage können Sie auch private Abfragegruppen erstellen.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Berichterstellung** | **Abfragen und Berichte**, und klicken Sie dann auf **Gruppenaktionen** | **Neue Gruppe**.

2 Geben Sie auf der Seite **Neue Gruppe** einen Gruppennamen ein.

3 Wählen Sie in **Gruppensichtbarkeit** eine der folgenden Optionen aus:

- **Private Gruppe** – Fügt die neue Gruppe unter **Eigene Gruppen** hinzu.
- **Öffentliche Gruppe** – Fügt die neue Gruppe unter **Freigegebene Gruppen** hinzu. In dieser Gruppe enthaltene Abfragen und Berichte können allen Benutzern angezeigt werden, die über Zugriff auf öffentliche Abfragen und Berichte verfügen.
- **Nach Berechtigungssatz freigegeben** – Fügt die neue Gruppe unter **Freigegebene Gruppen** hinzu. Auf Abfragen und Berichte in dieser Gruppe können nur Benutzer zugreifen, die den ausgewählten Berechtigungssätzen zugewiesen wurden.

Administratoren haben Vollzugriff auf alle Abfragen vom Typ Nach Berechtigungssatz und Öffentlich.

4 Klicken Sie auf **Speichern**.

Verschieben einer Abfrage in eine andere Gruppe

Ändern die Berechtigungen für eine Abfrage, indem Sie die Abfrage in eine andere Gruppe verschieben.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Berichterstellung** | **Abfragen und Berichte**. Wählen Sie in der Liste **Abfragen** die Abfrage aus, die Sie verschieben möchten.
2. Klicken Sie auf **Aktionen**, und wählen Sie eine der folgenden Optionen aus:
   - **In andere Gruppe verschieben** – Wählen Sie die Gruppe im Menü **Zielgruppe auswählen** aus.
   - **Duplizieren** – Geben Sie einen neuen Namen an, und wählen Sie die Gruppe im Menü **Gruppe, die Kopie erhält** aus.
3. Klicken Sie auf **OK**.

Exportieren und Importieren von Abfragen

Netzwerkinformationen sind sehr detailliert. Durch Exportieren und Importieren von einem Server auf einen anderen kann sichergestellt werden, dass der Datenabruf auf allen McAfee ePO-Servern konsistent erfolgt.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Öffnen Sie die Registerkarte Abfragen, indem Sie die folgenden Optionen auswählen: **Menü** | **Berichterstellung** | **Abfragen und Berichte**.
2. Wählen Sie eine der folgenden Aktionen aus:

Aktion	Vorgehensweise
Exportieren einer Abfrage	1 Wählen Sie in der Liste **Gruppen** die Gruppe aus, in der sich die Abfrage befindet, die Sie exportieren möchten, und wählen Sie dann die zu exportierende Abfrage aus. 2 Klicken Sie auf **Aktionen** | **Abfragen exportieren**. Vom McAfee ePO-Server wird eine XML-Datei an Ihren Browser gesendet. Von den meisten Browsern werden Sie standardmäßig zum Speichern der Datei aufgefordert. Die exportierte XML-Datei enthält eine vollständige Beschreibung aller Einstellungen, die zum Replizieren der exportierten Abfrage erforderlich sind.
Importieren einer Abfrage	1 Klicken Sie auf **Abfragen importieren**. 2 Klicken Sie auf **Durchsuchen**, und wählen Sie die XML-Datei aus, in der sich das zu importierende Dashboard befindet. 3 Wählen Sie eine neue oder eine vorhandene Gruppe für die Abfrage aus. • **Neu**: Geben Sie einen Namen für die Gruppe ein, und wählen Sie aus, ob sie privat oder öffentlich ist. • **Vorhanden**: Wählen Sie die Gruppe für die importierte Abfrage aus. 4 Klicken Sie auf **Speichern**. Es wird ein Bestätigungsbildschirm mit den Informationen zu der Abfrage aus der XML-Datei und ihrer Benennung nach dem Import angezeigt. Wenn die ausgewählte Datei keine gültige Abfrage enthält, wird eine Fehlermeldung angezeigt. 5 Klicken Sie auf **OK**, um den Importvorgang abzuschließen. Der neu importierten Abfrage werden die Berechtigungen der Gruppe zugewiesen, in die sie importiert wurde.

Exportieren von Abfrageergebnissen in andere Formate

Abfrageergebnisse können in die folgenden Formate exportiert werden: HTML, PDF, CSV und XML.

Das Exportieren von Abfrageergebnissen unterscheidet sich in mehreren Punkten vom Erstellen eines Berichts. Erstens werden zu der Ausgabe keine zusätzlichen Informationen hinzugefügt, wie es bei einem Bericht möglich ist. Eine Abfrage enthält nur die Ergebnisdaten. Außerdem werden mehrere Formate unterstützt. Es wird davon ausgegangen, dass exportierte Abfrageergebnisse weiter verarbeitet werden, deshalb werden Formate wie XML und CSV unterstützt. Berichte müssen vom Benutzer lesbar sein und werden daher nur als PDF-Dateien ausgegeben.

Im Gegensatz zu Abfrageergebnissen in der Konsole sind exportierte Daten nicht für Aktionen geeignet.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Berichterstellung** | **Abfragen und Berichte**, wählen Sie eine Abfrage aus, und klicken Sie dann auf **Ausführen**.

2 Nach der Ausführung der Abfrage klicken Sie auf**Optionen** | **Daten exportieren**.

Die Seite Exportieren wird angezeigt.

3 Wählen Sie aus, welche Elemente exportiert werden soll. Wählen Sie für diagrammbasierte Abfragen entweder **Nur Diagrammdaten** oder **Diagrammdaten und Aufgliederungstabellen** aus.

4 Legen Sie fest, ob die Datendateien einzeln oder in einer einzigen Archivdatei (ZIP) exportiert werden sollen.

5 Wählen Sie das Format der exportierten Datei aus.

- **CSV** – Verwenden Sie dieses Format, um die Daten in einer Tabellenkalkulationsanwendung (z. B. Microsoft Excel) zu verwenden.
- **XML** – Verwenden Sie dieses Format, um die Daten für andere Zwecke zu transformieren.
- **HTML**: Verwenden Sie dieses Berichtsformat, um die exportierten Ergebnisse als Webseite anzuzeigen.
- **PDF** – Verwenden Sie dieses Format, wenn Sie die Ergebnisse ausdrucken möchten.

6 Wenn Sie in eine PDF-Datei exportieren, müssen Sie Folgendes konfigurieren:

- Wählen Sie die **Seitengröße** und die **Seitenausrichtung** aus.
- (Optional) **Filterkriterien anzeigen**.
- (Optional) **Deckblatt mit folgendem Text hinzufügen**. Geben Sie den gewünschten Text ein.

7 Legen Sie fest, ob die Dateien als E-Mail-Anhänge an ausgewählte Empfänger gesendet oder in einem Speicherort auf dem Server gespeichert werden sollen, für den ein Link bereitgestellt wird. Die Datei können Sie öffnen oder an einem anderen Ort speichern, indem Sie mit der rechten Maustaste darauf klicken.

Beim Eingeben mehrerer E-Mail-Adressen für Empfänger müssen Sie die Einträge mit einem Komma oder Semikolon trennen.

8 Klicken Sie auf **Exportieren**.

Die Dateien werden entweder als E-Mail-Anhang an die Empfänger gesendet, oder es wird eine Seite aufgerufen, auf der Sie über Links auf die Dateien zugreifen können.

Zusammengefasste Abfragen mehrerer Server

ePolicy Orchestrator bietet die Möglichkeit zur Ausführung von Abfragen, bei denen ein Bericht mit einer Zusammenfassung von Daten aus mehreren Datenbanken erstellt wird.

Verwenden Sie diese Ergebnistypen im Assistenten des Abfragen-Generators für Abfragen dieses Typs:

- Zusammengefasste Bedrohungsereignisse
- Client-Ereignisse mit zusammengefassten Daten
- Compliance-Verlauf mit zusammengefassten Daten
- Verwaltete Systeme mit zusammengefassten Daten
- Zusammengefasste angewendete Richtlinien

Aktionsbefehle können nicht aus Ergebnistypen mit zusammengefassten Daten generiert werden.

Vorgehensweise

Zum Zusammenfassen von Daten, die in Abfragen mit zusammengefassten Daten verwendet werden sollen, müssen Sie jeden Server (einschließlich des lokalen Servers) registrieren, den Sie in die Abfrage einbeziehen möchten.

Nach der Registrierung der Server müssen Sie auf dem Berichterstellungs-Server (dem Server, auf dem die Berichterstellung für mehrere Server durchgeführt wird) Server-Tasks zum Zusammenfassen von Daten konfigurieren. Server-Tasks zum Zusammenfassen von Daten rufen Informationen aus allen in den Bericht einfließenden Datenbanken ab und füllen die "EPORollup_"-Tabellen auf dem Berichterstellungs-Server auf. Die Abfragen mit zusammengefassten Daten haben diese Datenbanktabellen auf dem Berichterstellungs-Server zum Ziel.

Vor dem Ausführen einer Compliance-Verlaufsabfrage mit zusammengefassten Daten müssen Sie auf jedem Server, dessen Daten in der Abfrage enthalten sein sollen, zwei vorbereitende Schritte ausführen:

- Erstellen einer Abfrage zum Definieren der Compliance
- Generieren eines Compliance-Ereignisses

Erstellen eines Server-Tasks zum Zusammenfassen von Daten

Server-Tasks zum Zusammenfassen von Daten beziehen Daten von mehreren Servern gleichzeitig.

Bevor Sie beginnen

Registrieren Sie alle McAfee ePO-Berichterstellungs-Server, die in Zusammenfassungsberichten enthalten sein sollen. Die einzelnen Server müssen registriert werden, um von diesen Servern zusammengefasste Daten zu sammeln, mit denen die EPORollup_-Tabellen des Zusammenfassungs-Berichterstellungs-Servers aufgefüllt werden.

Der Berichterstellungs-Server muss ebenfalls registriert werden, wenn seine zusammengefassten Daten in Zusammenfassungsberichten enthalten sein sollen.

Sie können nur Daten von registrierten McAfee ePO-Servern zusammenfassen, deren Versionen unterstützt werden. Sie können beispielsweise nicht Daten von McAfee ePO-Servern der Version 4.5 oder niedriger aggregieren.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Öffnen Sie den **Generator für Server-Tasks**.
   a Wählen Sie die folgenden Optionen aus: **Menü** | **Automatisierung** | **Server-Tasks**.
   b Klicken Sie auf **Neuer Task**.
2 Geben Sie auf der Seite **Beschreibung** einen Namen und eine Beschreibung für den Task ein, und legen Sie fest, ob er aktiviert werden soll. Klicken Sie anschließend auf **Weiter**.
3 Klicken Sie auf **Aktionen**, und wählen Sie **Daten zusammenfassen** aus.
4 Wählen Sie im Dropdown-Menü **Daten zusammenfassen von:** entweder **Allen registrierten Servern** oder **Ausgewählten registrierten Servern** aus.
5 Wenn Sie **Registrierte Server auswählen** ausgewählt haben, klicken Sie auf **Auswählen**. Wählen Sie im Dialogfeld **Registrierte Server auswählen** die Server aus, von denen Daten abgerufen werden sollen, und klicken Sie dann auf **OK**.

6 Wählen Sie die Datentypen aus, die zusammengefasst werden sollen, und klicken Sie dann auf **Weiter**. Wenn Sie mehrere Datentypen auswählen möchten, klicken Sie auf das Pluszeichen (**+**) am Ende der Tabellenüberschrift.

Die Datentypen Bedrohungsereignisse, Client-Ereignisse und Angewendete Richtlinien können noch weiter konfiguriert werden, sodass sie die Eigenschaften Bereinigen, Filter und Zusammenfassungsmethode enthalten. Klicken Sie dazu in der Zeile, in der die verfügbaren Eigenschaften beschrieben sind, auf **Konfigurieren**.

7 Planen Sie den Task, und klicken Sie dann auf **Weiter**.

Daraufhin wird die Seite Zusammenfassung angezeigt.

Falls Sie Berichte zu zusammengefassten Compliance-Verlaufsdaten erstellen, vergewissern Sie sich, dass die Zeiteinheit der Abfrage Compliance-Verlauf mit zusammengefassten Daten dem Planungstyp der Server-Tasks Compliance-Ereignis generieren auf den registrierten Servern entspricht.

8 Überprüfen Sie die Einstellungen, und klicken Sie dann auf **Speichern**.

Informationen zu Berichten

Berichte fassen Abfragen und andere Elemente in PDF-Dokumenten zusammen und stellen somit detaillierte Informationen für Analysen bereit.

Sie führen Berichte aus, um den Zustand Ihrer Umgebung zu ermitteln (z. B. Schwachstellen, Auslastung, Ereignisse usw.), sodass Sie die erforderlichen Änderungen vornehmen können, damit Ihre Umgebung sicher bleibt.

In Abfragen finden Sie ähnliche Informationen. Abfragen können Sie jedoch nur bei direkter Interaktion mit einem McAfee ePO-Server verwenden. In Berichten können Sie Informationen aus einer oder mehreren Abfragen in einem einzigen PDF-Dokument bündeln, wodurch eine zielgerichtete Analyse offline ermöglicht wird.

Als konfigurierbare Dokumente zeigen Berichte die Daten aus Abfragen von einer oder mehreren Datenbanken an. Im System wird jeweils das neueste Ergebnis für jeden Bericht gespeichert und zum Anzeigen zur Verfügung gestellt.

Den Zugriff auf Berichte können Sie mithilfe von Gruppen und Berechtigungssätzen auf die gleiche Weise wie bei Abfragen beschränken. Für Berichte und Abfragen können dieselben Gruppen verwendet werden, und da Berichte vor allem aus Abfragen bestehen, ist dadurch eine konsistente Zugriffssteuerung möglich.

Struktur von Berichten

Berichte enthalten eine Reihe von Elementen in einem Grundformat.

Auch wenn Berichte in hohem Maße angepasst werden können, weisen sie eine Grundstruktur auf, die die verschiedenen Elemente enthält.

Seitengröße und -ausrichtung

ePolicy Orchestrator unterstützt derzeit sechs Kombinationen von Seitengröße und -ausrichtung. Dazu gehören:

Seitengröße:

- US Letter (216 x 279 mm)
- US Legal (216 x 356 mm)
- A4 (210 x 297 mm)

Ausrichtung:

- Querformat
- Hochformat

Kopf- und Fußzeilen

Kopf- und Fußzeilen können ebenfalls in der Standardeinstellung verwendet oder vom Benutzer angepasst werden, auch mit Logos. Derzeit für Kopf- und Fußzeilen unterstützte Elemente sind:

- Logo
- Datum/Uhrzeit
- Seitennummer
- Benutzername
- Benutzerdefinierter Text

Seitenelemente

Seitenelemente bilden den Inhalt des Berichts. Sie können in beliebiger Reihenfolge kombiniert und nach Bedarf dupliziert werden. In ePolicy Orchestrator bereitgestellte Seitenelemente sind:

- Bilder
- Statischer Text
- Seitenumbrüche
- Abfragetabellen
- Abfragediagramme

Arbeiten mit Berichten

Berichte, die Abfragen und andere Elemente in detaillierten PDF-Dokumenten zusammenfassen, können erstellt, bearbeitet und verwaltet werden.

Diese Dokumente können eine große Menge nützlicher Daten liefern. Es sind jedoch einige Schritte erforderlich, um eine für Sie hilfreiche Datensammlung zu erstellen.

Aufgaben

- *Erstellen eines Berichts* auf Seite 283
  Sie können Berichte erstellen und diese in McAfee ePO speichern.
- *Bearbeiten eines vorhandenen Berichts* auf Seite 283
  Sie können den Inhalt oder die Präsentationsreihenfolge eines vorhandenen Berichts ändern.
- *Anzeigen von Berichtergebnissen* auf Seite 288
  Zeigen sie für jeden Bericht die zuletzt ausgeführte Version an.
- *Gruppieren von Berichten* auf Seite 288
  Jeder Bericht muss einer Gruppe zugewiesen sein.
- *Ausführen von Berichten* auf Seite 289
  Bevor Ergebnisse angezeigt werden können, müssen Berichte ausgeführt werden.
- *Planmäßiges Ausführen eines Berichts* auf Seite 289
  Erstellen Sie einen Server-Task, um einen Bericht automatisch auszuführen.
- *Exportieren und Importieren von Berichten* auf Seite 290
  Da Berichte mitunter sehr detaillierte Informationen enthalten, kann durch Exportieren und Importieren von einem Server auf einen anderen sichergestellt werden, dass der Datenabruf und die Berichterstellung auf allen McAfee ePO-Servern konsistent erfolgt.
- *Konfigurieren der Vorlage und des Speicherorts für exportierte Berichte* auf Seite 291
  Sie können das Erscheinungsbild und den Speicherort für Tabellen und Dashboards definieren, die Sie als Dokumente exportieren.
- *Löschen von Berichten* auf Seite 292
  Nicht mehr benötigte Berichte können gelöscht werden.

Erstellen eines Berichts

Sie können Berichte erstellen und diese in McAfee ePO speichern.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Berichterstellung** | **Abfragen und Berichte**, und wählen Sie dann die Registerkarte **Bericht** aus.
2. Klicken Sie auf **Neuer Bericht**.
3. Klicken Sie auf **Name, Beschreibung und Gruppe**. Geben Sie einen Namen und eine Beschreibung für den Bericht ein, und wählen Sie eine geeignete Gruppe aus. Klicken Sie auf **OK**.
4. Nun können Sie Elemente hinzufügen, entfernen und neu anordnen, Kopf- und Fußzeilen anpassen und das Seitenlayout ändern. Sie können jederzeit Ihren Fortschritt überprüfen, indem Sie auf **Ausführen** klicken.
5. Klicken Sie abschließend auf **Speichern**.

Bearbeiten eines vorhandenen Berichts

Sie können den Inhalt oder die Präsentationsreihenfolge eines vorhandenen Berichts ändern.

Wenn Sie einen neuen Bericht erstellen, gelangen Sie durch Klicken auf **Neuer Bericht** zu diesem Bildschirm.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Berichterstellung** | **Abfragen und Berichte**, und wählen Sie dann die Registerkarte **Bericht** aus.

2 Wählen Sie in der Liste einen Bericht aus, indem Sie das Kontrollkästchen neben dem entsprechenden Namen aktivieren.

3 Klicken Sie auf **Bearbeiten**.

Die Seite **Bericht-Layout** wird angezeigt.

Die folgenden Aufgaben können nun an dem Bericht durchgeführt werden.

Aufgaben

- *Hinzufügen von Elementen zu einem Bericht* auf Seite 284
  Sie können neue Elemente zu einem vorhandenen Bericht hinzufügen.
- *Konfigurieren von Bildelementen in Berichten* auf Seite 285
  Sie können neue Bilder hochladen und die in einem Bericht verwendeten Bilder ändern.
- *Konfigurieren von Textelementen in Berichten* auf Seite 285
  Sie können statischen Text in einen Bericht einfügen, um bestimmte Inhalte näher zu erklären.
- *Konfigurieren von Abfragetabellenelementen in Berichten* auf Seite 286
  Einige Abfragen sollten in Berichten in Tabellenform dargestellt werden.
- *Konfigurieren von Abfragediagrammelementen in Berichten* auf Seite 286
  Einige Abfragen sollten in Berichten in Diagrammform dargestellt werden.
- *Anpassen von Kopf- und Fußzeilen in Berichten* auf Seite 287
  Kopf- und Fußzeilen enthalten Informationen zu dem Bericht.
- *Entfernen von Elementen aus einem Bericht* auf Seite 287
  Wenn Elemente in einem Bericht nicht mehr benötigt werden, können Sie diese entfernen.
- *Ändern der Reihenfolge von Elementen in einem Bericht* auf Seite 288
  Sie können die Reihenfolge ändern, in der Elemente in einem Bericht angezeigt werden.

Hinzufügen von Elementen zu einem Bericht

Sie können neue Elemente zu einem vorhandenen Bericht hinzufügen.

Bevor Sie beginnen

Um diese Aktion durchführen zu können, muss ein Bericht auf der Seite **Bericht-Layout** geöffnet sein.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der **Toolbox** ein Element aus, und ziehen Sie es über das **Bericht-Layout**.

2 Legen Sie das Element dort an der gewünschten Stelle ab.

Bei anderen Berichtelementen als dem **Seitenumbruch** ist eine Konfiguration erforderlich. Die Konfigurationsseite für das Element wird angezeigt.

3 Klicken Sie nach Abschluss der Konfiguration des Elements auf **OK**.

Konfigurieren von Bildelementen in Berichten

Sie können neue Bilder hochladen und die in einem Bericht verwendeten Bilder ändern.

> **Bevor Sie beginnen**
> Es muss ein Bericht auf der Seite **Bericht-Layout** geöffnet sein.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Zum Konfigurieren eines bereits in einem Bericht vorhandenen Bildes klicken Sie auf den Pfeil in der linken oberen Ecke des Bildes. Klicken Sie auf **Konfigurieren**.

   Dadurch wird die Seite **Konfigurieren: Text** angezeigt. Wenn Sie ein Bild zum Bericht hinzufügen, wird die Seite **Konfigurieren: Bild** angezeigt, nachdem Sie das **Bild**-Element auf dem Bericht abgelegt haben.
2. Um ein vorhandenes Bild zu verwenden, wählen Sie es in der Galerie aus.
3. Um ein neues Bild zu verwenden, klicken Sie auf **Durchsuchen**, und wählen Sie das Bild auf Ihrem Computer aus. Klicken Sie auf **OK**.
4. Um eine bestimmte Bildbreite anzugeben, geben Sie den Wert in das Feld **Bildbreite** ein.

   In der Standardeinstellung wird das Bild ohne Größenänderung in seiner Originalbreite angezeigt, solange das Bild nicht breiter als die Seite ist. Falls das Bild breiter ist, wird es unter Beibehaltung des Seitenverhältnisses auf die verfügbare Breite verkleinert.
5. Legen Sie fest, ob das Bild links, rechts oder zentriert ausgerichtet werden soll.
6. Klicken Sie auf **OK**.

Konfigurieren von Textelementen in Berichten

Sie können statischen Text in einen Bericht einfügen, um bestimmte Inhalte näher zu erklären.

> **Bevor Sie beginnen**
> Es muss ein Bericht auf der Seite **Bericht-Layout** geöffnet sein.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Zum Konfigurieren eines bereits in einem Bericht vorhandenen Textes klicken Sie auf den Pfeil in der linken oberen Ecke des Textelements. Klicken Sie auf **Konfigurieren**.

   Dadurch wird die Seite **Konfigurieren: Text** angezeigt. Wenn Sie einen neuen Text zum Bericht hinzufügen, wird die Seite **Konfigurieren: Text** angezeigt, nachdem Sie das **Text**-Element auf dem Bericht abgelegt haben.
2. Sie können den vorhandenen Text im Bearbeitungsfeld **Text** bearbeiten oder neuen Text hinzufügen.
3. Bei Bedarf können Sie die Schriftgröße ändern.

   Der Standardwert ist Schriftgröße 12.
4. Wählen Sie die Textausrichtung aus: **Links**, **Zentriert** oder **Rechts**.
5. Klicken Sie auf **OK**.

Der von Ihnen eingegebene Text wird im Bericht-Layout innerhalb des Textelementes angezeigt.

Konfigurieren von Abfragetabellenelementen in Berichten

Einige Abfragen sollten in Berichten in Tabellenform dargestellt werden.

Bevor Sie beginnen

Es muss ein Bericht auf der Seite **Bericht-Layout** geöffnet sein.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Zum Konfigurieren einer bereits in einem Bericht vorhandenen Tabelle klicken Sie auf den Pfeil in der linken oberen Ecke der Tabelle. Klicken Sie auf **Konfigurieren**.

   Dadurch wird die Seite **Konfigurieren: Abfragetabelle** angezeigt. Wenn Sie eine Abfragetabelle zum Bericht hinzufügen, wird die Seite **Konfigurieren: Abfragetabelle** angezeigt, nachdem Sie das **Abfragetabellen**-Element auf dem Bericht abgelegt haben.

2. Wählen Sie in der Dropdown-Liste **Abfrage** eine Abfrage aus.

3. Wählen Sie in der Dropdown-Liste **Datenbank** die Datenbank aus, in der die Abfrage ausgeführt werden soll.

4. Wählen Sie die Schriftgröße aus, mit der die Tabellendaten angezeigt werden sollen.

   Der Standardwert ist Schriftgröße 8.

5. Klicken Sie auf **OK**.

Konfigurieren von Abfragediagrammelementen in Berichten

Einige Abfragen sollten in Berichten in Diagrammform dargestellt werden.

Bevor Sie beginnen

Es muss ein Bericht auf der Seite **Bericht-Layout** geöffnet sein.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Zum Konfigurieren eines bereits in einem Bericht vorhandenen Diagramms klicken Sie auf den Pfeil in der linken oberen Ecke des Diagramms. Klicken Sie auf **Konfigurieren**.

   Dadurch wird die Seite **Konfigurieren: Abfragediagramm** angezeigt. Wenn Sie ein Abfragediagramm zum Bericht hinzufügen, wird die Seite **Konfigurieren: Abfragediagramm** angezeigt, nachdem Sie das **Abfragetabellen**-Element auf dem Bericht abgelegt haben.

2. Wählen Sie in der Dropdown-Liste **Abfrage** eine Abfrage aus.

3. Legen Sie fest, ob nur das Diagramm, nur die Legende oder beides angezeigt werden soll.

4. Wenn sowohl das Diagramm als auch die Legende angezeigt werden sollen, müssen Sie auswählen, wie die beiden Elemente zueinander positioniert werden sollen.

5. Wählen Sie die Schriftgröße für die Legende aus.

   Der Standardwert ist Schriftgröße 8.

6. Wählen Sie die Bildhöhe für das Diagramm in Pixeln aus.

   Der Standardwert beträgt ein Drittel der Seitenhöhe.

7. Klicken Sie auf **OK**.

Anpassen von Kopf- und Fußzeilen in Berichten

Kopf- und Fußzeilen enthalten Informationen zu dem Bericht.

Innerhalb von Kopf- und Fußzeile gibt es sechs feste Positionen, an denen sich verschiedene Datenfelder befinden können. (Jeweils drei Positionen in der Kopfzeile und in der Fußzeile.)

Die Kopfzeile enthält ein links ausgerichtetes Logo und zwei übereinander angeordnete, rechts ausgerichtete Felder. Diese Felder können einen der vier folgenden Werte enthalten:

- Nichts
- Datum/Uhrzeit
- Seitennummer
- Benutzername des Benutzers, der den Bericht ausführt

Die Fußzeile verfügt ebenfalls über drei Felder: ein links ausgerichtetes, ein zentriertes ein rechts ausgerichtetes Feld. Diese drei Felder können einen der oben aufgeführten Werte oder auch benutzerdefinierten Text enthalten.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Berichterstellung** | **Abfragen**. Wählen Sie die Registerkarte **Bericht** aus.

2 Wählen Sie einen Bericht aus, und klicken Sie auf **Aktionen** | **Bearbeiten**.

3 Klicken Sie auf **Kopf- und Fußzeile**.

4 In der Standardeinstellung verwenden Berichte bei Kopf- und Fußzeilen die Systemeinstellung. Wenn dies nicht gewünscht wird, deaktivieren Sie **Standard-Server-Einstellung verwenden**.

   Zum Ändern der Systemeinstellungen für Kopf- und Fußzeilen klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie dann **Drucken und exportieren** aus, und klicken Sie auf **Bearbeiten**.

5 Zum Ändern des Logos klicken Sie auf **Logo bearbeiten**.

   a Wenn als Logo ein Text angezeigt werden soll, wählen Sie **Text** aus, und geben Sie dann den Text in das Bearbeitungsfeld ein.

   b Zum Hochladen eines neuen Logos wählen Sie **Bild** aus, wechseln dann auf Ihrem Computer zu dem Bild und wählen es aus und klicken anschließend auf **OK**.

   c Wenn Sie ein bereits hochgeladenes Logo verwenden möchten, wählen Sie es aus.

   d Klicken Sie auf **Speichern**.

6 Ändern Sie die Kopf- und Fußzeile gemäß den gewünschten Daten, und klicken Sie dann auf **OK**.

7 Klicken Sie auf **Speichern**, um die am Bericht vorgenommenen Änderungen zu speichern.

Entfernen von Elementen aus einem Bericht

Wenn Elemente in einem Bericht nicht mehr benötigt werden, können Sie diese entfernen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Berichterstellung** | **Abfragen und Berichte**, und wählen Sie dann die Registerkarte **Bericht** aus.

2 Wählen Sie einen Bericht aus, und klicken Sie auf **Aktionen** | **Bearbeiten**.

3 Klicken Sie in der linken oberen Ecke des zu löschenden Elements auf den Pfeil und anschließend auf **Entfernen**.

Das Element wird aus dem Bericht gelöscht.

4 Klicken Sie auf **Speichern**, um die am Bericht vorgenommenen Änderungen zu speichern.

Ändern der Reihenfolge von Elementen in einem Bericht

Sie können die Reihenfolge ändern, in der Elemente in einem Bericht angezeigt werden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Berichterstellung** | **Abfragen und Berichte**, und wählen Sie dann die Registerkarte **Bericht** aus.

2 Wählen Sie in der Liste einen Bericht aus, und klicken Sie auf **Aktionen** | **Bearbeiten**.

3 Klicken Sie zum Verschieben eines Elements auf dessen Titelleiste, und ziehen Sie es an eine neue Position.

Die Elementpositionierung unter dem gezogenen Element ändert sich, während Sie den Cursor im Bericht bewegen. Wenn sich der Cursor über einer nicht zulässigen Position befindet, werden auf jeder Seite des Berichts rote Balken angezeigt.

4 Lassen Sie den Cursor los, wenn sich das Element an der gewünschten Position befindet.

5 Klicken Sie auf **Speichern**, um die am Bericht vorgenommenen Änderungen zu speichern.

Anzeigen von Berichtergebnissen

Zeigen sie für jeden Bericht die zuletzt ausgeführte Version an.

Die Ergebnisse für einen Bericht werden bei jedem Ausführen auf dem Server gespeichert und in der Berichtsliste angezeigt.

Bei jedem Ausführen eines Berichts werden die vorherigen Ergebnisse gelöscht und können nicht mehr abgerufen werden. Wenn Sie die unterschiedlichen Durchläufe desselben Berichts vergleichen möchten, sollten Sie die Ergebnisse anderweitig archivieren.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Berichterstellung** | **Abfragen und Berichte**, und wählen Sie dann die Registerkarte **Bericht** aus.

2 In der Berichtsliste sehen Sie eine Spalte **Ergebnis der letzten Ausführung**. Jeder Eintrag in dieser Spalte ist ein Link zu der PDF-Datei, die beim letzten erfolgreichen Ausführen des Berichts erstellt wurde. Klicken Sie zum Abrufen eines Berichts auf einen Link in dieser Spalte.

Eine PDF-Datei wird in Ihrem Browser geöffnet. Ihr Browser verhält sich dabei so, wie Sie es für diesen Dateityp konfiguriert haben.

Gruppieren von Berichten

Jeder Bericht muss einer Gruppe zugewiesen sein.

Berichte werden beim Erstellen einer Gruppe zugewiesen. Diese Zuweisung kann jedoch zu einem späteren Zeitpunkt geändert werden. Meist werden Berichte gruppiert, um ähnliche Berichte zusammenzufassen oder um Berechtigungen für bestimmte Berichte zu verwalten.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Berichterstellung** | **Abfragen und Berichte**, und wählen Sie dann die Registerkarte **Bericht** aus.
2. Wählen Sie einen Bericht aus, und klicken Sie auf **Aktionen** | **Bearbeiten**.
3. Klicken Sie auf **Name, Beschreibung und Gruppe**.
4. Wählen Sie in der Dropdown-Liste **Berichtsgruppe** einen Bericht aus, und klicken Sie auf **OK**.
5. Klicken Sie auf **Speichern**, um am Bericht vorgenommene Änderungen zu speichern.

Wenn Sie die gewünschte Gruppe in der Liste **Gruppen** im linken Bereich des Berichtsfensters auswählen, wird der Bericht in der Berichtsliste angezeigt.

Ausführen von Berichten

Bevor Ergebnisse angezeigt werden können, müssen Berichte ausgeführt werden.

Berichte können in ePolicy Orchestrator in drei unterschiedlichen Speicherorten ausgeführt werden:

- In der Berichtsliste
- In einem Server-Task
- Auf der Seite **Bericht-Layout** beim Erstellen eines neuen oder Bearbeiten eines vorhandenen Berichts

Hier wird das Ausführen von Berichten in der Berichtsliste erläutert.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Berichterstellung** | **Abfragen und Berichte**, und wählen Sie dann die Registerkarte **Bericht** aus.
2. Wählen Sie einen Bericht in der Berichtliste aus, und klicken Sie dann auf **Aktionen** | **Ausführen**.

   Nach Abschluss des Berichts wird die erstellte PDF an Ihren Browser gesendet. Je nach Ihren Browser-Einstellungen wird der Bericht entweder angezeigt oder heruntergeladen.

Die Berichterstellung kann mitunter einige Zeit dauern. Zwar können mehrere Berichte gleichzeitig ausgeführt, jedoch immer nur ein Bericht über die Benutzeroberfläche erstellt werden. Wenn der Bericht fertig gestellt ist, wird die Spalte **Ergebnis der letzten Ausführung** in der Berichtsliste mit einem Link zu der PDF-Datei aktualisiert, in der sich diese Ergebnisse befinden.

Planmäßiges Ausführen eines Berichts

Erstellen Sie einen Server-Task, um einen Bericht automatisch auszuführen.

Wenn Sie einen Bericht ohne manuelles Eingreifen ausführen möchten, nutzen Sie am besten einen Server-Task. Mit der hier beschriebenen Vorgehensweise erstellen Sie einen Server-Task, der automatische, geplante Ausführungen eines bestimmten Berichts ermöglicht.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Öffnen Sie den Generator für Server-Tasks.

   a Wählen Sie auf der Seite Abfragen und Berichte einen Bericht aus.

   b Wählen Sie die folgenden Optionen aus: **Aktionen** | **Plan**.

2 Geben Sie einen Namen und eine Beschreibung für den Task ein, und weisen Sie einen Planungsstatus zu. Klicken Sie dann auf **Weiter**.

   Wenn der Task automatisch ausgeführt werden soll, legen Sie den **Planungsstatus** auf **Aktiviert** fest.

3 Wählen Sie in der Dropdown-Liste **Aktionen** den Eintrag **Bericht ausführen** aus. Wählen Sie den auszuführenden Bericht sowie die Zielsprache aus, und klicken Sie dann auf **Weiter**.

4 Wählen Sie einen Planungstyp (Häufigkeit) und Zeitpunkte (Datum und Uhrzeit) für die Ausführung des Berichts aus, und klicken Sie dann auf **Weiter**.

   Die Planungsinformationen werden nur verwendet, wenn Sie **Planungsstatus** aktivieren.

5 Klicken Sie auf **Speichern**, um den Server-Task zu speichern.

Der neue Task wird nun in der Liste **Server-Tasks** angezeigt.

Exportieren und Importieren von Berichten

Da Berichte mitunter sehr detaillierte Informationen enthalten, kann durch Exportieren und Importieren von einem Server auf einen anderen sichergestellt werden, dass der Datenabruf und die Berichterstellung auf allen McAfee ePO-Servern konsistent erfolgt.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Öffnen Sie die Seite **Berichte**: Wählen Sie **Menü** | **Berichterstellung** | **Abfragen und Berichte** und dann die Registerkarte **Berichte** aus.

2 Wählen Sie eine der folgenden Aktionen aus:

Aktion	Vorgehensweise
Exportieren von Berichten	1 Wählen Sie in der Liste **Gruppen** die Gruppe aus, in der sich der Bericht befindet, den Sie exportieren möchten. 2 Wählen Sie den zu exportierenden Bericht aus, und klicken Sie dann auf **Aktionen** | **Berichte exportieren**. Vom McAfee ePO-Server wird eine XML-Datei an Ihren Browser gesendet. Von den meisten Browsern werden Sie standardmäßig zum Speichern der Datei aufgefordert. Der exportierte Bericht enthält die Definitionen aller im Bericht enthaltenen Elemente. Dazu gehören u. a. externe Datenbankdefinitionen, Abfragen und Grafiken.
Importieren eines Berichts	1 Klicken Sie auf der Seite Bericht auf **Berichte importieren**. 2 Klicken Sie auf **Durchsuchen**, und wählen Sie die XML-Datei aus, in der sich der zu importierende Bericht befindet. 3 Wählen Sie eine neue oder eine vorhandene Gruppe für den Bericht aus. • **Neu**: Geben Sie einen Namen für die Gruppe ein, und wählen Sie aus, ob sie privat oder öffentlich ist. • **Vorhanden**: Wählen Sie die Gruppe für den importierten Bericht aus. 4 Klicken Sie auf **OK**. 5 Klicken Sie auf **Importieren**, um den Importvorgang abzuschließen. Dem neu importierten Bericht werden die Berechtigungen der Gruppe zugewiesen, in die er importiert wurde.

Konfigurieren der Vorlage und des Speicherorts für exportierte Berichte

Sie können das Erscheinungsbild und den Speicherort für Tabellen und Dashboards definieren, die Sie als Dokumente exportieren.

Mit der Server-Einstellung **Drucken und exportieren** können Sie Folgendes konfigurieren:

- Kopf- und Fußzeilen, einschließlich Name, Seitenzahl, eines benutzerdefinierten Logos usw.
- Seitengröße und -ausrichtung zum Drucken
- Das Verzeichnis, in dem exportierte Tabellen und Dashboards gespeichert werden

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, und wählen Sie dann in der Liste **Einstellungskategorien** den Eintrag **Drucken und exportieren** aus.

2 Klicken Sie auf **Bearbeiten**. Die Seite **Drucken und exportieren: Bearbeiten** wird angezeigt.

3 Klicken Sie im Abschnitt **Kopf- und Fußzeilen für exportierte Dokumente** auf **Logo bearbeiten**, um die Seite **Logo bearbeiten** zu öffnen.

   a Wählen Sie **Text** aus, und geben Sie den Text ein, der in der Dokumentkopfzeile angezeigt werden soll, oder führen Sie einen der folgenden Schritte aus:

      - Wählen Sie **Bild** aus, und wechseln Sie zu der Bilddatei (z. B. zur Datei mit Ihrem Firmenlogo).
      - Wählen Sie das McAfee-Standardlogo aus.

   b Klicken Sie auf **OK**, um zur Seite **Drucken und exportieren: Bearbeiten** zurückzukehren.

4 Wählen Sie in den Dropdown-Listen die gewünschten Metadaten aus, die in der Kopf- und der Fußzeile angezeigt werden sollen.

5 Wählen Sie eine **Seitengröße** und eine **Seitenausrichtung** aus.

6 Geben Sie einen neuen Speicherort ein, oder übernehmen Sie den Standardspeicherort, in dem exportierte Dokumente gespeichert werden.

7 Klicken Sie auf **Speichern**.

Löschen von Berichten

Nicht mehr benötigte Berichte können gelöscht werden.

> **Bevor Sie beginnen**
> Zum Löschen eines Berichts müssen Sie Bearbeitungsberechtigungen für den Bericht besitzen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Berichterstellung** | **Abfragen und Berichte**, und wählen Sie dann die Registerkarte **Bericht** aus.

2 Wählen Sie in der Liste der Berichte einen oder mehrere Berichte zum Löschen aus.

3 Klicken Sie auf **Aktionen** | **Löschen**. Wenn Sie sicher sind, dass die Aktion durchgeführt werden soll, klicken Sie auf **Ja**.

Die Berichte wurden gelöscht. Server-Tasks, die auf gelöschte Berichte verweisen, sind nicht mehr gültig.

22 Ereignisse und Antworten

Sie können den McAfee ePO-Server so konfigurieren, dass bei Bedrohungs-, Client- oder Server-Ereignissen eine Antwort ausgelöst wird.

Inhalt

- *Verwenden automatischer Antworten*
- *Beschränkung, Aggregation und Gruppierung*
- *Standardregeln*
- *Planen von Antworten*
- *Erstmaliges Konfigurieren von Antworten*
- *Bestimmen, wie Ereignisse weitergeleitet werden*
- *Konfigurieren automatischer Antworten*
- *Bestimmen der an den Server weiterzuleitenden Ereignisse*
- *Auswählen eines Intervalls für Benachrichtigungsereignisse*
- *Erstellen und Bearbeiten von Regeln für automatische Antworten*
- *Fragen zu Ereignissen und Antworten*

Verwenden automatischer Antworten

Für welche Ereignistypen Sie automatische Antworten konfigurieren können, hängt davon ab, welche Software-Produkte mit dem McAfee ePO-Server verwaltet werden.

In der Standardeinstellung kann eine Antwort folgende Aktionen beinhalten:

- Das Erstellen von Problemen
- Das Ausführen von Server-Tasks
- Das Ausführen externer Befehle
- Das Ausführen von Systembefehlen
- Das Senden von E-Mail-Nachrichten
- Das Senden von SNMP-Traps

Es lässt sich genau konfigurieren, bei welchen Ereignissen aus welchen Kategorien Benachrichtigungen generiert und mit welcher Häufigkeit diese Benachrichtigungen gesendet werden sollen.

Diese Funktion dient dazu, benutzerdefinierte Benachrichtigungen und Aktionen für die Fälle zu erstellen, in denen die Bedingungen einer Regel erfüllt sind. Zu diesen Bedingungen gehören u. a.:

- Die Erkennung von Bedrohungen durch Ihre Antiviren-Software. Es werden zwar viele Antivirenprodukte unterstützt, bei VirusScan Enterprise jedoch beinhalten Ereignisse auch die IP-Adresse der Angriffsquelle, sodass das System, das die übrige Umgebung infiziert, isoliert werden kann.
- Virenausbruch. Zum Beispiel, wenn innerhalb von fünf Minuten 1.000 Ereignisse vom Typ "Virus entdeckt" empfangen werden.
- Hohe Übereinstimmung mit McAfee ePO-Server-Ereignissen. Zum Beispiel ein Fehler bei einer Repository-Aktualisierung oder einem Replizierungs-Task.

Beschränkung, Aggregation und Gruppierung

Durch Festlegen von Schwellenwerten, die auf Aggregation, Beschränkung und Gruppierung basieren, können Sie konfigurieren, wann Benachrichtigungen gesendet werden.

Aggregation

Mit der Aggregation können Sie Schwellenwerte für Ereignisse festlegen, ab denen die Regel eine Benachrichtigung sendet. Konfigurieren Sie eine Regel zum Beispiel so, dass eine Benachrichtigung gesendet wird, wenn der Server innerhalb einer Stunde 1.000 Virusentdeckungen von unterschiedlichen Systemen oder 100 Virusentdeckungen von einem System empfängt.

Beschränkung

Wenn Sie eine Regel konfiguriert haben, nach der Sie bei einem möglichen Virenausbruch benachrichtigt werden, können Sie mit der Beschränkung sicherstellen, dass Sie nicht zu viele Benachrichtigungen erhalten. Als Administrator eines umfangreichen Netzwerks erhalten Sie möglicherweise Zehntausende Ereignisse innerhalb einer Stunde, was bei einer solchen Regel zu Tausenden von Benachrichtigungen führen würde. Mithilfe von Antworten können Sie die Anzahl der Benachrichtigungen beschränken, die Sie aufgrund einer einzelnen Regel erhalten. Sie können beispielsweise in derselben Regel bestimmen, dass Sie lediglich eine Benachrichtigung pro Stunde erhalten möchten.

Gruppierung

Mittels Gruppierung können Sie mehrere aggregierte Ereignisse zusammenfassen. So können zum Beispiel Ereignisse mit dem gleichen Schweregrad in einer einzigen Gruppe zusammengefasst werden. Durch eine Gruppierung kann der Administrator auf alle Ereignisse mit diesem oder einem höheren Schweregrad gleichzeitig reagieren. Außerdem können Sie damit auch für die bei verwalteten Systemen oder Servern generierten Ereignisse Prioritäten vergeben.

Standardregeln

Aktivieren Sie die ePolicy Orchestrator-Standardregeln, um die Funktion zum Ausprobieren sofort verwenden zu können.

Vor dem Aktivieren von Standardregeln sollten Sie die folgenden Schritte ausführen:

- Geben Sie den E-Mail-Server an (unter **Menü** | **Konfiguration** | **Server-Einstellungen**), von dem die Benachrichtigungsmeldungen gesendet werden.
- Vergewissern Sie sich, dass Sie die E-Mail-Adresse der Person angeben, die E-Mail-Benachrichtigungen empfangen soll. Diese Adresse wird im Assistenten auf der Seite **Aktionen** festgelegt.

Tabelle 22-1 Standardbenachrichtigungsregeln

Regelname	Zugehörige Ereignisse	Konfigurationen
Fehler beim Aktualisieren oder Replizieren des verteilten Repositorys	Fehler beim Aktualisieren oder Replizieren des verteilten Repositorys	Sendet eine Benachrichtigung, wenn bei einer Aktualisierung oder einer Replizierung ein Fehler auftritt.
Malware entdeckt	Ereignisse von unbekannten Produkten	Sendet eine Benachrichtigung: • Die Anzahl der Ereignisse erreicht innerhalb einer Stunde mindestens den Wert 1.000. • Eine Benachrichtigung wird max. alle zwei Stunden gesendet. • Sofern vorhanden und zusammen mit vielen anderen Parametern werden die IP-Adresse des Quellsystems, die Bezeichnung für die aktuelle Bedrohung und Informationen zum aktuellen Produkt mitgesendet. • Die Anzahl ausgewählter eindeutiger Werte beträgt 500.
Fehler beim Aktualisieren oder Replizieren des Master-Repositorys	Fehler beim Aktualisieren oder Replizieren des Master-Repositorys	Sendet eine Benachrichtigung, wenn bei einer Aktualisierung oder einer Replizierung ein Fehler auftritt.
Nicht konformer Computer entdeckt	Ereignisse vom Typ Nicht konformer Computer entdeckt	Sendet eine Benachrichtigung, wenn ein Ereignis vom Server-Task Compliance-Ereignis generieren empfangen wird.

Planen von Antworten

Wenn Sie die folgenden Punkte gut planen, bevor Sie Benachrichtigungsregeln erstellen, können Sie Zeit sparen.

Stellen Sie sicher, dass Sie über einen Plan zu den folgenden Punkten verfügen:

- Ereignistypen und -gruppen (Produkt und Server), die in Ihrer Umgebung Benachrichtigungen auslösen.
- Wer sollte welche Benachrichtigungen erhalten? So ist es zum Beispiel nicht notwendig, den Administrator von Gruppe B über eine fehlgeschlagene Replizierung in Gruppe A zu informieren, es sollten aber alle Administratoren informiert werden, wenn in Gruppe A eine infizierte Datei entdeckt wurde.
- Welche Arten und Ebenen von Grenzwerten möchten Sie für jede Regel festlegen? Eventuell möchten Sie zum Beispiel während eines Virenausbruchs nicht bei jeder infizierten Datei eine E-Mail-Benachrichtigung erhalten. Stattdessen können Sie auswählen, dass Ihnen eine solche Benachrichtigung unabhängig von der Anzahl der vom Server empfangenen Ereignisse höchstens alle fünf Minuten zugesendet wird.
- Welche Befehle oder registrierten ausführbaren Dateien sollen ausgeführt werden, wenn die Bedingungen einer Regel erfüllt sind?
- Welcher Server-Task soll ausgeführt werden, wenn die Bedingungen einer Regel erfüllt sind?

Erstmaliges Konfigurieren von Antworten

Gehen Sie wie nachfolgend allgemein beschrieben vor, wenn Sie zum ersten Mal Ereignisse und automatische Antworten konfigurieren.

Wenn Sie zum ersten Mal eine Regel für automatische Antworten erstellen, sollten Sie die folgenden Punkte beachten:

1 Machen Sie sich mit automatischen Antworten und deren Funktionsweise in der Systemstruktur und im Netzwerk vertraut.

2 Planen Sie die Implementierung. Welche Benutzer müssen über welche Ereignisse informiert werden?

3 Bereiten Sie die Komponenten und Berechtigungen vor, die im Zusammenhang mit automatischen Antworten benötigt werden. Dazu gehören:

- **Berechtigungen für automatische Antworten** – Erstellen oder bearbeiten Sie Berechtigungssätze, und stellen Sie sicher, dass diese den entsprechenden McAfee ePO-Benutzern zugewiesen sind.
- **E-Mail-Server** – Konfigurieren Sie den E-Mail-Server (SMTP) unter **Server-Einstellungen**.
- **Liste der E-Mail-Kontakte** – Geben Sie unter **Kontakte** die Liste an, aus der Sie Empfänger für Benachrichtigungen auswählen.
- **Registrierte ausführbare Dateien** – Geben Sie eine Liste mit registrierten ausführbaren Dateien an, die ausgeführt werden sollen, wenn die Bedingungen einer Regel erfüllt sind.
- **Server-Tasks** – Erstellen Sie Server-Tasks, die infolge einer Antwortregel als Aktion ausgeführt werden sollen.
- **SNMP-Server** – Geben Sie eine Liste von SNMP-Servern an, die beim Erstellen von Regeln verwendet werden sollen. Sie können Regeln konfigurieren, um SNMP-Traps an SNMP-Server zu senden, wenn die Bedingungen zum Erstellen einer Benachrichtigung erfüllt sind.

Bestimmen, wie Ereignisse weitergeleitet werden

Legen Sie fest, wann Ereignisse weitergeleitet und welche Ereignisse sofort weitergeleitet werden sollen.

Der Server empfängt Ereignisbenachrichtigungen von Agenten. Sie können McAfee Agent-Richtlinien so konfigurieren, dass Ereignisse entweder sofort oder nur in Agent-zu-Server-Kommunikationsintervallen zum Server gesendet werden.

Wenn Sie auswählen, dass Ereignisse sofort gesendet werden sollen (Standard), leitet der McAfee Agent alle Ereignisse sofort bei Erhalt weiter.

Das Standardintervall für die Verarbeitung von Ereignisbenachrichtigungen beträgt eine Minute. Daher kann es zu einer Verzögerung kommen, bevor Ereignisse verarbeitet werden. Das Standardintervall können Sie in den Server-Einstellungen für Ereignisbenachrichtigungen (**Menü** | **Konfiguration** | **Server-Einstellungen**) ändern.

Wenn nicht alle Ereignisse sofort gesendet werden sollen, leitet der McAfee Agent nur solche Ereignisse unverzüglich weiter, die vom ausstellenden Produkt mit einer hohen Priorität gekennzeichnet wurden. Andere Ereignisse werden nur bei der Agent-zu-Server-Kommunikation gesendet.

Aufgaben

- *Bestimmen der sofort weiterzuleitenden Ereignisse* auf Seite 297
  Legen Sie fest, ob Ereignisse unverzüglich oder nur bei Agent-zu-Server-Kommunikationen weitergeleitet werden sollen.
- *Bestimmen der weiterzuleitenden Ereignisse* auf Seite 297
  Mithilfe der Seite **Server-Einstellungen** können Sie bestimmen, welche Ereignisse an den Server weitergeleitet werden.

Bestimmen der sofort weiterzuleitenden Ereignisse

Legen Sie fest, ob Ereignisse unverzüglich oder nur bei Agent-zu-Server-Kommunikationen weitergeleitet werden sollen.

Wenn für die aktuell angewendete Richtlinie nicht festgelegt ist, dass Ereignisse sofort hochzuladen sind, müssen Sie entweder die aktuell angewendete Richtlinie ändern oder eine neue McAfee Agent-Richtlinie erstellen. Diese Einstellung ist auf der Seite **Bedrohungsereignisprotokoll** konfiguriert.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Richtlinie** | **Richtlinienkatalog**, und wählen Sie dann in der Dropdown-Liste **Produkt** den Eintrag **McAfee Agent** und in der Dropdown-Liste **Kategorie** den Eintrag **Allgemein** aus.
2. Klicken Sie auf eine vorhandene Agenten-Richtlinie.
3. Aktivieren Sie auf der Registerkarte **Ereignisse** die Option **Weiterleiten von Ereignissen nach Priorität aktivieren**.
4. Wählen Sie den Ereignisschweregrad aus.

   Ereignisse des ausgewählten Schweregrades (und höher) werden sofort an den Server weitergeleitet.
5. Geben Sie ein **Intervall zwischen Uploads** (in Minuten) ein, um die Häufigkeit des anfallenden Datenverkehrs zu regulieren.
6. Geben Sie die **Maximale Anzahl von Ereignissen pro Upload** ein, um den Umfang des anfallenden Datenverkehrs zu begrenzen.
7. Klicken Sie auf **Speichern**.

Bestimmen der weiterzuleitenden Ereignisse

Mithilfe der Seite **Server-Einstellungen** können Sie bestimmen, welche Ereignisse an den Server weitergeleitet werden.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie **Ereignisfilterung** aus, und klicken Sie dann auf **Bearbeiten**.
2. Wählen Sie die Ereignisse aus, und klicken Sie dann auf **Speichern**.

Diese Einstellungen werden wirksam, sobald sich sämtliche Agenten beim Server gemeldet haben.

Konfigurieren automatischer Antworten

Konfigurieren Sie die erforderlichen Ressourcen, mit denen Sie die automatischen Antworten optimal nutzen können.

Aufgaben

- *Zuweisen von Berechtigungen für Benachrichtigungen* auf Seite 298
  Mit Berechtigungen für Benachrichtigungen können Benutzer registrierte ausführbare Dateien anzeigen, erstellen und bearbeiten.
- *Zuweisen von Berechtigungen für automatische Antworten* auf Seite 299
  Mit Berechtigungen für Antworten können Benutzer Antwortregeln für unterschiedliche Ereignistypen und Gruppen erstellen.
- *Verwalten von SNMP-Servern* auf Seite 299
  Konfigurieren Sie Antworten zur Verwendung Ihres SNMP-Servers (Simple Network Management Protocol).
- *Verwalten registrierter ausführbare Dateien und externer Befehle* auf Seite 301
  Die von Ihnen konfigurierten registrierten ausführbaren Dateien werden ausgeführt, wenn die Bedingungen einer Regel erfüllt sind. Die Befehle zum Ausführen der registrierten ausführbaren Dateien werden von automatischen Antworten ausgelöst.

Zuweisen von Berechtigungen für Benachrichtigungen

Mit Berechtigungen für Benachrichtigungen können Benutzer registrierte ausführbare Dateien anzeigen, erstellen und bearbeiten.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Benutzerverwaltung** | **Berechtigungssätze**, und erstellen Sie dann entweder einen Berechtigungssatz, oder wählen Sie einen vorhandenen Berechtigungssatz aus.

2 Klicken Sie neben **Ereignisbenachrichtigungen** auf **Bearbeiten**.

3 Wählen Sie die gewünschte Berechtigung für Benachrichtigungen aus:

- **Keine Berechtigungen**
- **Registrierte ausführbare Dateien anzeigen**
- **Registrierte ausführbare Dateien erstellen und bearbeiten**
- **Regeln und Benachrichtigungen für gesamte Systemstruktur anzeigen (setzt Zugriffsberechtigungen für Systemstrukturgruppe außer Kraft)**

4 Klicken Sie auf **Speichern**.

5 Wenn Sie einen Berechtigungssatz erstellt haben, klicken Sie auf **Menü** | **Benutzerverwaltung** | **Benutzer**.

6 Wählen Sie einen Benutzer aus, dem Sie den neuen Berechtigungssatz zuweisen möchten, und klicken Sie dann auf **Bearbeiten**.

7 Aktivieren Sie neben **Berechtigungssätze** das Kontrollkästchen für den Berechtigungssatz mit den gewünschten Berechtigungen für Benachrichtigungen, und klicken Sie dann auf **Speichern**.

Zuweisen von Berechtigungen für automatische Antworten

Mit Berechtigungen für Antworten können Benutzer Antwortregeln für unterschiedliche Ereignistypen und Gruppen erstellen.

Zum Erstellen einer Antwortregel müssen Benutzer über Berechtigungen für die folgenden Funktionen verfügen.

- Bedrohungsereignisprotokoll
- Systemstruktur
- Server-Tasks
- Entdeckte Systeme

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Benutzerverwaltung** | **Berechtigungssätze**, und erstellen Sie dann entweder einen Berechtigungssatz, oder wählen Sie einen vorhandenen Berechtigungssatz aus.

2 Klicken Sie neben **Automatische Antwort** auf **Bearbeiten**.

3 Wählen Sie eine Berechtigung für **Automatische Antwort** aus:

- **Keine Berechtigungen**
- **Antworten anzeigen; Ergebnisse zu Antworten im Server-Task-Protokoll anzeigen**
- **Antworten erstellen, bearbeiten, anzeigen und abbrechen; Ergebnisse zu Antworten im Server-Task-Protokoll anzeigen**

4 Klicken Sie auf **Speichern**.

5 Wenn Sie einen Berechtigungssatz erstellt haben, klicken Sie auf **Menü** | **Benutzerverwaltung** | **Benutzer**.

6 Wählen Sie einen Benutzer aus, dem Sie den neuen Berechtigungssatz zuweisen möchten, und klicken Sie dann auf **Bearbeiten**.

7 Aktivieren Sie neben **Berechtigungssätze** das Kontrollkästchen für den Berechtigungssatz mit den gewünschten Berechtigungen für **Automatische Antwort**, und klicken Sie dann auf **Speichern**.

Verwalten von SNMP-Servern

Konfigurieren Sie Antworten zur Verwendung Ihres SNMP-Servers (Simple Network Management Protocol).

Sie können das Antwortsystem so konfigurieren, dass SNMP-Traps an Ihren SNMP-Server gesendet werden. Auf diese Weise können Sie SNMP-Traps an der gleichen Stelle empfangen, an der Sie Ihre Netzwerkverwaltungs-Software zum Anzeigen von detaillierten Informationen über die Systeme in Ihrer Umgebung verwenden.

Weitere Konfigurationsschritte oder das Starten eines Diensts zum Konfigurieren dieser Funktion sind nicht erforderlich.

Aufgaben

- *Bearbeiten von SNMP-Servern* auf Seite 300
  Bearbeiten Sie Einträge zu vorhandenen SNMP-Servern.
- *Löschen eines SNMP-Servers* auf Seite 300
  Löschen Sie einen SNMP-Server aus der Liste **Registrierte Server**.

Bearbeiten von SNMP-Servern

Bearbeiten Sie Einträge zu vorhandenen SNMP-Servern.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Konfiguration** | **Registrierte Server**.
2. Wählen Sie in der Liste der registrierten Server einen SNMP-Server aus, und klicken Sie dann auf **Aktionen** | **Bearbeiten**.
3. Bearbeiten Sie nach Bedarf die Server-Einstellungen, und klicken Sie dann auf **Speichern**.

Löschen eines SNMP-Servers

Löschen Sie einen SNMP-Server aus der Liste **Registrierte Server**.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Konfiguration** | **Registrierte Server**.
2. Wählen Sie in der Liste der registrierten Server einen SNMP-Server aus, und klicken Sie dann auf **Aktionen** | **Löschen**.
3. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Ja**.

Der SNMP-Server wird aus der Liste **Registrierte Server** entfernt.

Importieren von MIB-Dateien

Importieren Sie MIB-Dateien, bevor Sie Regeln einrichten, nach denen Benachrichtigungen mithilfe einer SNMP-Trap an einen SNMP-Server gesendet werden.

Sie müssen drei MIB-Dateien aus dem Ordner `\Programme\McAfee\ePolicy Orchestrator\MIB` importieren. Die Dateien müssen in der folgenden Reihenfolge importiert werden:

1. NAI-MIB.MIB
2. TVD-MIB.MIB
3. EPO-MIB.MIB

Mithilfe dieser Dateien können Sie über Ihr Netzwerkverwaltungsprogramm die in den SNMP-Traps enthaltenen Daten in Klartext decodieren. Die Datei EPO-MIB.MIB ist zum Definieren der folgenden Traps von den anderen beiden Dateien abhängig:

- **epoThreatEvent** – Dieser Trap wird gesendet, wenn eine automatische Antwort für ein McAfee ePO-Bedrohungsereignis ausgelöst wird. Er enthält Variablen, die mit den Eigenschaften des Bedrohungsereignisses übereinstimmen.
- **epoStatusEvent** – Dieser Trap wird gesendet, wenn eine automatische Antwort für ein McAfee ePO-Statusereignis ausgelöst wird. Er enthält Variablen, die mit den Eigenschaften eines (Server-)Statusereignisses übereinstimmen.
- **epoClientStatusEvent** – Dieser Trap wird gesendet, wenn eine automatische Antwort für ein McAfee ePO-Client-Statusereignis ausgelöst wird. Er enthält Variablen, die mit den Eigenschaften eines Client-Statusereignisses übereinstimmen.
- **epoTestEvent** – Dies ist ein Test-Trap, der gesendet wird, wenn Sie auf den Seiten "SNMP-Server: Neu" oder "SNMP-Server: Bearbeiten" auf **Test-Trap senden** klicken.

Weitere Anweisungen zum Importieren und Implementieren von MIB-Dateien finden Sie in der Dokumentation Ihres Netzwerkverwaltungsprogramms.

Verwalten registrierter ausführbare Dateien und externer Befehle

Die von Ihnen konfigurierten registrierten ausführbaren Dateien werden ausgeführt, wenn die Bedingungen einer Regel erfüllt sind. Die Befehle zum Ausführen der registrierten ausführbaren Dateien werden von automatischen Antworten ausgelöst.

Sie können Befehle für registrierte ausführbare Dateien können Sie nur in Konsolenanwendungen ausführen.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Konfiguration** | **Registrierte ausführbare Dateien**.

2 Wählen Sie eine der folgenden Aktionen aus.

Aktion	Vorgehensweise
Hinzufügen einer registrierten ausführbaren Datei	1 Klicken Sie auf **Aktionen** | **Registrierte ausführbare Datei**. 2 Geben Sie einen Namen für die registrierte ausführbare Datei ein. 3 Geben Sie den Pfad ein, und wählen Sie die gewünschte registrierte ausführbare Datei aus, die von einer Regel ausgeführt werden soll, wenn diese ausgelöst wird. 4 Falls erforderlich, ändern Sie die Benutzeranmeldeinformationen. 5 Testen Sie die ausführbare Datei, und prüfen Sie dies im **Audit-Protokoll** nach. 6 Klicken Sie auf **Speichern**. Die neue registrierte ausführbare Datei wird in der Liste **Registrierte ausführbare Dateien** angezeigt.
Bearbeiten einer registrierten ausführbaren Datei	1 Suchen Sie auf der Seite **Registrierte ausführbare Datei** die Datei, die Sie bearbeiten möchten, und klicken Sie auf **Bearbeiten**. 2 Nehmen Sie die gewünschten Änderungen vor, und klicken Sie dann auf **Speichern**.
Duplizieren einer registrierten ausführbaren Datei	1 Suchen Sie auf der Seite **Registrierte ausführbare Datei** die Datei, die Sie duplizieren möchten, und klicken Sie auf **Duplizieren**. 2 Geben Sie einen Namen für die registrierte ausführbare Datei ein, und klicken Sie dann auf **OK**. Die duplizierte registrierte ausführbare Datei wird in der Liste **Registrierte ausführbare Dateien** angezeigt.
Löschen einer registrierten ausführbaren Datei	1 Suchen Sie auf der Seite **Registrierte ausführbare Datei** die Datei, die Sie löschen möchten, und klicken Sie auf **Löschen**. 2 Wenn Sie dazu aufgefordert werden, klicken Sie auf **OK**. Die gelöschte registrierte ausführbare Datei wird in der Liste **Registrierte ausführbare Dateien** nicht mehr aufgeführt.

Bestimmen der an den Server weiterzuleitenden Ereignisse

Mittels **Server-Einstellungen** und **Ereignisfilterung** können Sie bestimmen, welche Ereignisse an den Server weitergeleitet werden sollen.

Bevor Sie beginnen

Diese Einstellungen wirken sich darauf aus, wie viel Bandbreite in Ihrer Umgebung belegt wird und welche Ergebnisse ereignisbasierte Abfragen zurückgeben.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie **Ereignisfilterung** aus, und klicken Sie dann unten auf der Seite auf **Bearbeiten**. Die Seite **Ereignisfilterung: Bearbeiten** wird angezeigt.
2. Wählen Sie die Ereignisse aus, die der Agent an den Server weiterleiten soll, und klicken Sie dann auf **Speichern**.

Änderungen an diesen Einstellungen werden wirksam, nachdem alle Agenten mit dem McAfee ePO-Server kommuniziert haben.

Auswählen eines Intervalls für Benachrichtigungsereignisse

Mit dieser Einstellung wird festgelegt, wie oft ePO-Benachrichtigungsereignisse an das System für automatische Antworten gesendet werden.

Es gibt drei Typen von Benachrichtigungsereignissen:

- **Client-Ereignisse** – Das sind Ereignisse, die auf verwalteten Systemen auftreten. Zum Beispiel Produktaktualisierung erfolgreich durchgeführt.
- **Bedrohungsereignisse** – Das sind Ereignisse, die anzeigen, dass eine potenzielle Bedrohung entdeckt wurde. Zum Beispiel Virus entdeckt.
- **Server-Ereignisse** – Das sind Ereignisse, die auf dem Server auftreten. Zum Beispiel Fehler bei Repository-Abruf.

Eine automatische Antwort kann nur dann ausgelöst werden, wenn das System für automatische Antworten eine Benachrichtigung erhalten hat. McAfeeEs wird empfohlen, ein relativ kurzes Intervall für das Senden dieser Benachrichtigungsereignisse anzugeben. McAfeeAußerdem wird empfohlen, ein Testintervall festzulegen, das kurz genug ist, sodass das System für automatische Antworten möglichst zeitnah auf ein Ereignis reagieren kann, jedoch nicht zu kurz, damit nicht unnötig Bandbreite belegt wird.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste **Einstellungskategorien** den Eintrag **Ereignisbenachrichtigungen** aus, und klicken Sie dann auf **Bearbeiten**.
2. Geben Sie für das **Testintervall** (das standardmäßig 1 Minute beträgt) einen Wert zwischen 1 und 9.999 Minuten an, und klicken Sie dann auf **Speichern**.

Erstellen und Bearbeiten von Regeln für automatische Antworten

Definieren Sie, wann und wie eine Antwort auf ein Ereignis erfolgen soll, das auf einem Server oder einem verwalteten System auftritt.

Regeln für automatische Antworten weisen keine abhängige Reihenfolge auf.

Aufgaben

- *Beschreiben einer Regel* auf Seite 303
  Beim Erstellen einer neuen Regel können Sie eine Beschreibung hinzufügen, die Sprache festlegen, die Gruppe und den Typ des Ereignisses angeben, das die Antwort auslöst, sowie die Regel aktivieren oder deaktivieren.
- *Festlegen von Filtern für die Regel* auf Seite 303
  Sie können im Assistenten **Antwort-Generator** auf der Seite **Filter** die Filter für die Antwortregel festlegen.
- *Festlegen von Schwellenwerten für die Regel* auf Seite 304
  Auf der Seite **Aggregation** des Assistenten **Antwort-Generator** legen Sie fest, wann die Regel von dem Ereignis ausgelöst wird.
- *Konfigurieren der Aktion für Regeln zu automatischen Antworten* auf Seite 304
  Sie können die Antworten, die von der Regel ausgelöst werden, im **Antwort-Generator** auf der Seite **Antworten** konfigurieren.

Beschreiben einer Regel

Beim Erstellen einer neuen Regel können Sie eine Beschreibung hinzufügen, die Sprache festlegen, die Gruppe und den Typ des Ereignisses angeben, das die Antwort auslöst, sowie die Regel aktivieren oder deaktivieren.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Automatisierung** | **Automatische Antworten**, und klicken Sie dann auf **Aktionen** | **Neue Antwort** oder neben einer Regel auf **Bearbeiten**.

2 Geben Sie auf der Seite **Beschreibung** einen eindeutigen Namen und mögliche Anmerkungen zu der Regel ein.

Regelnamen müssen auf einem Server eindeutig sein. Wenn zum Beispiel ein Benutzer eine Regel namens `Notfallbenachrichtigung` erstellt, darf kein anderer Benutzer eine Regel mit dem gleichen Namen erstellen.

3 Wählen Sie im Menü **Sprache** die Sprache für die Regel aus.

4 Wählen Sie die **Ereignisgruppe** und den **Ereignistyp** aus, von denen die Antwort ausgelöst wird.

5 Wählen Sie neben **Status** aus, ob die Regel **Aktiviert** oder **Deaktiviert** ist.

6 Klicken Sie auf **Weiter**.

Festlegen von Filtern für die Regel

Sie können im Assistenten **Antwort-Generator** auf der Seite **Filter** die Filter für die Antwortregel festlegen.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Wählen Sie in der Liste **Verfügbare Eigenschaften** eine Eigenschaft aus, und geben Sie den Wert an, nach dem das Ergebnis der Antwort gefiltert werden soll.

> **Verfügbare Eigenschaften** richtet sich danach, welcher Ereignistyp und welche Ereignisgruppe auf der Seite **Beschreibung** des Assistenten ausgewählt sind.

2 Klicken Sie auf **Weiter**.

Festlegen von Schwellenwerten für die Regel

Auf der Seite **Aggregation** des Assistenten **Antwort-Generator** legen Sie fest, wann die Regel von dem Ereignis ausgelöst wird.
Schwellenwerte von Regeln sind eine Kombination von Aggregation, Beschränkung und Gruppierung.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Aktivieren Sie neben **Aggregation** die Option **Diese Antwort für jedes Ereignis auslösen**, oder wählen Sie die Option **Diese Antwort auslösen beim Auftreten mehrerer Ereignisse in** aus, und legen Sie einen entsprechenden Zeitraum fest. In letzterem Fall geben Sie den Zeitraum in Minuten, Stunden oder Tagen an.

2 Wenn Sie die Option **Diese Antwort auslösen beim Auftreten mehrerer Ereignisse in** ausgewählt haben, können Sie festlegen, dass eine Antwort ausgelöst werden soll, wenn die angegebenen Bedingungen erfüllt sind. Diese Bedingungen sind eine beliebige Kombination der folgenden beiden Punkte:

- **Die Anzahl eindeutiger Werte für eine Ereigniseigenschaft erreicht einen Mindestwert.** Diese Bedingung wird verwendet, wenn ein bestimmter Wert für das Auftreten der Ereigniseigenschaft ausgewählt ist.
- **Wenn mindestens die folgende Anzahl von Ereignissen aufgetreten ist.** Geben Sie eine bestimmte Anzahl von Ereignissen ein.

> Sie können eine oder beide Optionen auswählen. So können Sie die Regel zum Beispiel so festlegen, dass diese Antwort ausgelöst werden soll, wenn die ausgewählte Ereigniseigenschaft mehr als 300 Mal auftritt, oder wenn die Anzahl der Ereignisse den Wert 3.000 überschreitet, je nachdem, welcher Schwellenwert zuerst überschritten wird.

3 Wählen Sie neben **Gruppierung** aus, ob die aggregierten Ereignisse gruppiert werden sollen. Wenn Sie festlegen, dass die aggregierten Ereignisse gruppiert werden sollen, müssen Sie angeben, nach welcher Eigenschaft des Ereignisses die Gruppierung erfolgen soll.

4 Aktivieren Sie neben **Beschränkung** gegebenenfalls die Option **Diese Antwort nicht häufiger auslösen als alle**, und legen Sie einen Zeitraum fest, nach dessen Verstreichen die Regel wieder Benachrichtigungen senden darf.

Der Zeitraum kann in Minuten, Stunden oder Tagen angegeben werden.

5 Klicken Sie auf **Weiter**.

Konfigurieren der Aktion für Regeln zu automatischen Antworten

Sie können die Antworten, die von der Regel ausgelöst werden, im **Antwort-Generator** auf der Seite **Antworten** konfigurieren.
Mithilfe der Schaltflächen **+** und **-** neben der Dropdown-Liste für den Benachrichtigungstyp können Sie die Regel so konfigurieren, dass sie mehrere Aktionen auslöst.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Wenn die Benachrichtigung in Form einer E-Mail- oder Text-Pager-Nachricht gesendet werden soll, wählen Sie in der Dropdown-Liste **E-Mail senden** aus.

   a Klicken Sie neben **Empfänger** auf die Schaltfläche zum Durchsuchen (…), und wählen Sie die Empfänger für die Nachricht aus. Diese Liste der verfügbaren Empfänger stammt aus den Kontakten (**Menü** | **Benutzerverwaltung** | **Kontakte**). Alternativ dazu können Sie die E-Mail-Adressen auch manuell eingeben, getrennt durch ein Komma.

   b Wählen Sie die Wichtigkeit der Benachrichtigungs-E-Mail aus.

   c Geben Sie den **Betreff** für die Nachricht ein. Optional können Sie auch jede verfügbare Variable direkt in die Betreffzeile eingeben.

   d Geben Sie den Text ein, der im **Nachrichtentext** der Nachricht angezeigt werden soll. Optional können Sie auch jede verfügbare Variable direkt in den Textteil eingeben.

   e Klicken Sie abschließend auf **Weiter** oder auf **+**, um eine weitere Benachrichtigung hinzuzufügen.

2 Wenn die Benachrichtigung in Form eines SNMP-Traps gesendet werden soll, wählen Sie in der Dropdown-Liste **SNMP-Trap senden** aus.

   a Wählen Sie einen SNMP-Server aus der Dropdown-Liste aus.

   b Wählen Sie den Typ des Werts aus, der in dem SNMP-Trap gesendet werden soll.

   - **Wert**
   - **Anzahl eindeutiger Werte**
   - **Liste eindeutiger Werte**
   - **Liste aller Werte**

   Nicht alle Ereignisse beinhalten diese Informationen. Wenn zu einigen der von Ihnen ausgewählten Optionen nichts angezeigt wird, dann steht diese Information in der Ereignisdatei nicht zur Verfügung.

   c Klicken Sie abschließend auf **Weiter** oder auf **+**, um eine weitere Benachrichtigung hinzuzufügen.

3 Wenn Sie möchten, dass die Benachrichtigung einen externen Befehl ausführt, wählen Sie in der Dropdown-Liste **Externen Befehl ausführen** aus.

   a Wählen Sie Dateien unter **Registrierte ausführbare Dateien** aus, und geben Sie etwaige **Argumente** für den Befehl ein.

   b Klicken Sie abschließend auf **Weiter** oder auf **+**, um eine weitere Benachrichtigung hinzuzufügen.

4 Wenn Sie möchten, dass die Benachrichtigung ein Problem erstellt, wählen Sie in der Dropdown-Liste **Problem erstellen** aus.

   a Wählen Sie den Typ des zu erstellenden Problems aus.

   b Geben Sie einen eindeutigen Namen und eventuelle Anmerkungen zu dem Problem ein. Optional können Sie auch jede der verfügbaren Variablen direkt in den Namen und die Beschreibung einfügen.

   c Wählen Sie in den entsprechend Dropdown-Listen den **Zustand**, die **Priorität**, den **Schweregrad** und die **Lösung** für das Problem aus.

   d Geben Sie den Namen des Beauftragten in das Textfeld ein.

   e Klicken Sie abschließend auf **Weiter** oder auf **+**, um eine weitere Benachrichtigung hinzuzufügen.

5 Wenn Sie möchten, dass die Benachrichtigung einen geplanten Task ausführt, wählen Sie in der Dropdown-Liste **Server-Task ausführen** aus.

   a Wählen Sie in der Dropdown-Liste **Auszuführender Task** den Task aus, der ausgeführt werden soll.

   b Klicken Sie abschließend auf **Weiter** oder auf **+**, um eine weitere Benachrichtigung hinzuzufügen.

6 Überprüfen Sie die Informationen auf der Seite Zusammenfassung, und klicken Sie dann auf **Speichern**.

Die neue Antwortregel wird in der Liste **Antworten** angezeigt.

Fragen zu Ereignissen und Antworten

Wenn ich eine Antwortregel für Virenfunde erstelle, erhalte ich dann für jedes Ereignis während eines Virenausbruchs eine Benachrichtigung?

Nein. Regeln können so konfiguriert werden, dass eine Benachrichtigung entweder erst beim Auftreten einer bestimmten Anzahl von Ereignissen innerhalb eines bestimmten Zeitraums gesendet wird oder dass höchstens eine Benachrichtigung innerhalb eines definierten Zeitraums gesendet wird.

Kann ich eine Regel erstellen, die Benachrichtigungen für mehrere Empfänger generiert?

Ja. Sie können mehrere E-Mail-Adressen für Empfänger im Assistenten Antwort-Generator eingeben.

Kann ich eine Regel erstellen, die mehrere Benachrichtigungstypen generiert?

Ja. ePolicy Orchestrator Benachrichtigungen unterstützen jede Kombination der folgenden Benachrichtigungsziele für jede Regel:

- E-Mail (einschließlich Standard-SMTP, SMS und Text-Pager)
- SNMP-Server (mithilfe von SNMP-Traps)
- Externe, auf dem McAfee ePO-Server installierte Tools
- Probleme
- Geplante Server-Tasks

23 Probleme

Bei Problemen handelt es sich um Aktionselemente, die priorisiert, zugewiesen und nachverfolgt werden können.

Inhalt

- *Beschreibung und Funktionsweise von Problemen*
- *Arbeiten mit Problemen*
- *Bereinigen abgeschlossener Probleme*

Beschreibung und Funktionsweise von Problemen

Die Art und Weise der Problemverwaltung wird von Benutzern mit den entsprechenden Berechtigungen und durch die installierten verwalteten Produkterweiterungen definiert.

Der Zustand, die Priorität, der Schweregrad, die Lösung, der Beauftragte und das Fälligkeitsdatum von Problemen werden von Benutzern definiert und können jederzeit geändert werden. Auf der Seite **Automatische Antworten** können Sie auch Standardantworten auf Probleme angeben. Diese Standardwerte werden basierend auf einer vom Benutzer konfigurierten Antwort automatisch angewendet, wenn ein Problem erstellt wird. Durch Antworten können auch mehrere Ereignisse in einem einzigen Problem aggregiert werden, sodass es zu keiner Überlastung des McAfee ePO-Servers mit zu vielen Problemen kommt.

Probleme können manuell gelöscht werden. Abgeschlossene Probleme können basierend auf ihrem Alter sowohl manuell als auch durch einen vom Benutzer konfigurierten Server-Task automatisch entfernt werden.

Arbeiten mit Problemen

Sie können Probleme erstellen, zuweisen, im Detail anzeigen, bearbeiten, löschen und bereinigen.

Aufgaben

- *Manuelles Erstellen von einfachen Problemen* auf Seite 308
  Einfache Probleme können manuell erstellt werden. Komplexere Probleme müssen automatisch erstellt werden.
- *Konfigurieren von Antworten zum automatischen Erstellen von Problemen* auf Seite 309
  Verwenden Sie Antworten, damit beim Eintreten bestimmter Ereignisse automatisch Probleme erstellt werden.
- *Verwalten von Problemen* auf Seite 309
  Sie können Probleme zuweisen, löschen, bearbeiten, ihre Details anzeigen und ihnen Anmerkungen hinzufügen.

Manuelles Erstellen von einfachen Problemen

Einfache Probleme können manuell erstellt werden. Komplexere Probleme müssen automatisch erstellt werden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Automatisierung** | **Probleme**, und klicken Sie dann auf **Aktionen** | **Neues Problem**.

2 Wählen Sie im Dialogfeld **Neues Problem** in der Dropdown-Liste **Problem vom folgenden Typ erstellen** den Typ **Einfach** aus, und klicken Sie dann auf **OK**.

3 Konfigurieren Sie das neue Problem.

Option	Aktion
Name	Geben Sie einen eindeutigen Namen für das Problem ein.
Beschreibung	Geben Sie eine eindeutige Beschreibung des Problems ein.
Zustand	Weisen Sie dem Problem einen Zustand zu: • Unbekannt • Neu • Zugewiesen • Gelöst • Abgeschlossen
Priorität	Weisen Sie dem Problem eine Priorität zu: • Unbekannt • Am niedrigsten • Niedrig • Mittel • Hoch • Am höchsten
Schweregrad	Weisen Sie dem Problem einen Schweregrad zu: • Unbekannt • Am niedrigsten • Niedrig • Mittel • Hoch • Am höchsten
Lösung	Weisen Sie dem Problem eine Lösung zu. Die Problemlösung kann erneut zugewiesen werden, sobald das Problem verarbeitet wird: • Keine • Behoben • Entfällt • Kann nicht behoben werden
Beauftragter	Geben Sie den Benutzernamen der Person ein, der das Problem zugewiesen wurde, oder wählen Sie die Person aus, indem Sie auf die Schaltfläche zum Durchsuchen […] klicken.
Fälligkeitsdatum	Legen Sie fest, ob das Problem ein Fälligkeitsdatum aufweisen soll. Falls ja, weisen Sie ein Datum und eine Uhrzeit für die Fälligkeit des Problems zu. In der Vergangenheit liegende Fälligkeitsdaten sind nicht zulässig.

4 Klicken Sie auf **Speichern**.

Konfigurieren von Antworten zum automatischen Erstellen von Problemen

Verwenden Sie Antworten, damit beim Eintreten bestimmter Ereignisse automatisch Probleme erstellt werden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Öffnen Sie den Antwort-Generator.
   a. Wählen Sie die folgenden Optionen aus: **Menü** | **Automatisierung** | **Automatische Reaktionen**.
   b. Klicken Sie auf **Neue Reaktion**.
2. Füllen Sie die Felder aus, und klicken Sie dann auf **Weiter**.
3. Wählen Sie Eigenschaften aus, um die Ereignisse einzugrenzen, bei denen diese Antwort ausgelöst wird, und klicken Sie dann auf **Weiter**.
4. Geben Sie die zusätzlichen Details an, und klicken Sie dann auf **Weiter**.
   - Gibt an, wie häufig Ereignisse eintreten müssen, damit eine Reaktion generiert wird.
   - Eine Methode zum Gruppieren von Ereignissen.
   - Gibt an, wie lange diese Reaktion erfolgen soll.
5. Wählen Sie **Problem erstellen** in der Dropdown-Liste aus, und wählen Sie dann den Typ für das zu erstellende Problem aus.

   Diese Auswahl bestimmt die Optionen, die auf dieser Seite angezeigt werden.
6. Geben Sie einen Namen und eine Beschreibung für das Problem ein. Wählen Sie bei Bedarf eine oder mehrere Variablen für den Namen und die Beschreibung aus.

   Diese Funktion stellt eine Reihe von Variablen bereit, die Informationen enthalten, die bei der Behebung des Problems hilfreich sein können.
7. Geben Sie gegebenenfalls weitere Optionen für die Antwort ein, oder wählen Sie sie aus. Klicken Sie dann auf **Weiter**.
8. Überprüfen Sie die Einzelheiten zur Konfiguration der Antwort, und klicken Sie dann auf **Speichern**.

Verwalten von Problemen

Sie können Probleme zuweisen, löschen, bearbeiten, ihre Details anzeigen und ihnen Anmerkungen hinzufügen.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Automatisierung** | **Probleme**.
2. Führen Sie die gewünschten Aufgaben aus.

Option	Beschreibung
Hinzufügen von Kommentaren zu Problemen	1 Aktivieren Sie das Kontrollkästchen neben jedem Problem, das Sie kommentieren möchten, und klicken Sie dann auf **Aktionen** | **Kommentar hinzufügen**. 2 Geben Sie im Bereich **Kommentar hinzufügen** den Kommentar ein, der zu den ausgewählten Problemen hinzugefügt werden soll. 3 Klicken Sie auf **OK**, um den Kommentar hinzuzufügen.
Zuweisen von Problemen	Aktivieren Sie das Kontrollkästchen neben jedem Problem, das Sie zuweisen möchten, und klicken Sie dann auf **Einem Benutzer zuweisen**.
Anzeigen erforderlicher Spalten auf der Seite Probleme	Klicken Sie auf **Aktionen** | **Spalten auswählen**. Hier können Sie die Spalten mit Daten auswählen, die auf der Seite Probleme angezeigt werden sollen.
Löschen von Problemen	1 Aktivieren Sie das Kontrollkästchen neben jedem Problem, das Sie löschen möchten, und klicken Sie dann auf **Löschen**. 2 Klicken Sie im Bereich **Aktion** auf **OK**, um die ausgewählten Probleme zu löschen.
Bearbeiten von Problemen	1 Aktivieren Sie das Kontrollkästchen neben einem Problem, und klicken Sie dann auf **Bearbeiten**. 2 Nehmen Sie die gewünschten Änderungen am Problem vor. 3 Klicken Sie auf **Speichern**.
Exportieren der Liste von Problemen	Klicken Sie auf **Aktionen** | **Tabelle exportieren**. Die Seite Exportieren wird geöffnet. Auf der Seite Exportieren können Sie das Format der zu exportierenden Dateien, die Art der Komprimierung (z. B. in einer ZIP-Datei) und die weitere Vorgehensweise (z. B. per E-Mail als Anhang senden) angeben.
Anzeigen von Problemdetails	Klicken Sie auf ein Problem. Die Seite Problem: Details wird angezeigt. Auf dieser Seite werden alle Einstellungen für das Problem sowie das Problemaktivitätsprotokoll angezeigt.

Bereinigen abgeschlossener Probleme

Sie können abgeschlossene Probleme in der Datenbank bereinigen, um sie dauerhaft zu löschen.

Aufgaben

- *Manuelles Bereinigen abgeschlossener Probleme* auf Seite 310
  Durch regelmäßiges Bereinigen abgeschlossener Probleme in der Datenbank wird diese nicht zu voll.
- *Planmäßiges Bereinigen abgeschlossener Probleme* auf Seite 311
  Sie können einen Task planen, mit dem Sie regelmäßig abgeschlossene Probleme aus der Datenbank bereinigen. Durch Bereinigen abgeschlossener Probleme können Sie die Größe der Datenbank reduzieren.

Manuelles Bereinigen abgeschlossener Probleme

Durch regelmäßiges Bereinigen abgeschlossener Probleme in der Datenbank wird diese nicht zu voll.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Automatisierung** | **Probleme**, und klicken Sie dann auf **Aktionen** | **Bereinigen**.
2. Geben Sie im Dialogfeld **Bereinigen** eine Zahl ein, und wählen Sie dann eine Zeiteinheit aus.
3. Klicken Sie auf **OK**, um abgeschlossene Probleme zu bereinigen, die älter als das angegebene Datum sind.

Diese Funktion wirkt sich nicht nur auf die abgeschlossenen Probleme in der aktuellen Ansicht sondern auf alle abgeschlossenen Probleme aus.

Planmäßiges Bereinigen abgeschlossener Probleme

Sie können einen Task planen, mit dem Sie regelmäßig abgeschlossene Probleme aus der Datenbank bereinigen. Durch Bereinigen abgeschlossener Probleme können Sie die Größe der Datenbank reduzieren.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Öffnen Sie den **Generator für Server-Tasks**.
   a. Wählen Sie die folgenden Optionen aus: **Menü** | **Automatisierung** | **Server-Tasks**.
   b. Klicken Sie auf **Neuer Task**.
2. Geben Sie einen Namen und eine Beschreibung für den Server-Task ein.
3. Aktivieren oder deaktivieren Sie den Plan für den Server-Task.
   Der Server-Task wird erst ausgeführt, nachdem er aktiviert wurde.
4. Klicken Sie auf **Weiter**.
5. Wählen Sie in der Dropdown-Liste die Option **Abgeschlossene Probleme bereinigen** aus.
6. Geben Sie eine Zahl ein, und wählen Sie dann eine Zeiteinheit aus.
7. Klicken Sie auf **Weiter**.
8. Planen Sie den Server-Task, und klicken Sie dann auf **Weiter**.
9. Überprüfen Sie die Einzelheiten zur Konfiguration des Server-Tasks, und klicken Sie dann auf **Speichern**.

Die abgeschlossenen Probleme werden zum Zeitpunkt des geplanten Tasks bereinigt.

24 Wiederherstellung nach Systemausfall

Mit der Funktion Wiederherstellung nach Systemausfall können Sie ePolicy Orchestrator schnell wiederherstellen oder erneut installieren. Bei der Funktion **Wiederherstellung nach Systemausfall** werden mithilfe einer Snapshot-Funktion die ePolicy Orchestrator-Konfiguration sowie Erweiterungen, Schlüssel und andere Informationen in regelmäßigen Abständen in Snapshot-Datensätzen in der ePolicy Orchestrator-Datenbank gespeichert.

Inhalt

- *Was ist eine Wiederherstellung nach einem Systemausfall?*
- *Komponenten für die Wiederherstellung nach einem Systemausfall*
- *Funktionsweise der Wiederherstellung nach einem Systemausfall*
- *Erstellen eines Snapshots*
- *Konfigurieren von Server-Einstellungen zur Wiederherstellung nach einem Systemausfall*

Was ist eine Wiederherstellung nach einem Systemausfall?

Die ePolicy Orchestrator-Funktion für Wiederherstellungen nach einem Systemausfall speichert bestimmte Datenbankeinträge zum McAfee ePO-Server mithilfe von Snapshots in der Microsoft SQL Server-Datenbank von ePolicy Orchestrator.

Die von den Snapshots gespeicherten Datensätze enthalten die gesamte zum Zeitpunkt der Snapshot-Erstellung vorliegende ePolicy Orchestrator-Konfiguration. Sobald die Snapshot-Datensätze in der Datenbank gespeichert sind, können Sie mithilfe der Microsoft SQL Server-Sicherungsfunktion die gesamte ePolicy Orchestrator-Datenbank speichern und zwecks Wiederherstellung von ePolicy Orchestrator auf einem anderen SQL-Server wiederherstellen.

Beispiele für Verbindungen der SQL-Wiederherstellungs-Datenbank

Mithilfe des wiederhergestellten ePolicy Orchestrator-SQL-Datenbank-Servers, auf dem sich der Snapshot für die Wiederherstellung nach einem Systemausfall befindet, können Sie eine Verbindung zu folgenden Servern herstellen:

- Wiederhergestellte McAfee ePO-Server-Hardware mit dem ursprünglichen Server-Namen und der ursprünglichen IP-Adresse – Dadurch haben Sie zum Beispiel die Möglichkeit, ePolicy Orchestrator nach einem fehlgeschlagenen Upgrade wiederherzustellen.
- Neue McAfee ePO-Server-Hardware mit dem ursprünglichen Server-Namen und der ursprünglichen IP-Adresse – Dadurch können Sie Server-Hardware problemlos aufrüsten oder wiederherstellen, um dann schnell die Verwaltung Ihrer Netzwerksysteme wieder aufzunehmen.

- Neue McAfee ePO-Server-Hardware mit einem neuen Server-Namen und einer neuen IP-Adresse – Auf diese Weise können Sie zum Beispiel Ihren Server aus einer Domäne in eine andere verschieben.

  Dieses Beispiel ist auch als vorübergehende Lösung für die Netzwerkverwaltung geeignet, während Sie die McAfee ePO-Server-Hardware und -Software wieder zurück in die ursprüngliche Domäne verschieben und dort installieren.

- Wiederhergestellte oder neue McAfee ePO-Server-Hardware mit mehreren Netzwerkkarten – Dabei müssen Sie darauf achten, dass für die Netzwerkkarte des McAfee ePO-Servers die korrekte IP-Adresse konfiguriert ist.

Der Snapshot-Vorgang ist je nach Version Ihrer SQL-Datenbank so konfiguriert, dass er täglich automatisch ausgeführt wird. Durch Konfiguration eines Skripts, mit dem die SQL-Sicherung automatisch ausgeführt und die SQL-Sicherungsdatei auf den SQL-Datenbank-Wiederherstellungs-Server kopiert wird, können Sie Ihren McAfee ePO-Server noch einfacher wiederherstellen. Darüber hinaus können Sie Snapshots auch manuell erstellen oder Skripte manuell ausführen, um ePolicy Orchestrator nach komplizierten oder wichtigen Änderungen schnell zu sichern.

Mit dem Monitor der Snapshots zur Wiederherstellung nach einem Systemausfall im ePolicy Orchestrator-Dashboard können Sie Ihre Snapshots zentral verwalten und überwachen.

Komponenten für die Wiederherstellung nach einem Systemausfall

Für die Wiederherstellung nach einem Systemausfall von ePolicy Orchestrator sind bestimmte Anforderungen hinsichtlich der Hard- und Software, der Zugriffsberechtigungen sowie der Informationen zu beachten.

Sie benötigen zwei Server-Hardware-Plattformen:

- Ihre vorhandene McAfee ePO-Server-Hardware (nachfolgend als "primärer" McAfee ePO-Server bezeichnet).
- Eine duplizierte SQL-Server-Hardware (nachfolgend als "Wiederherstellungs"-Server bezeichnet), auf der eine zur primären McAfee ePO-Server-Datenbank passende Version von Microsoft SQL Server ausgeführt wird. Dieser Wiederherstellungs-Server sollte mittels Snapshot- und Microsoft SQL-Sicherungsprozessen immer auf dem aktuellsten Konfigurationsstand des primären McAfee ePO-Servers und der SQL-Datenbank gehalten werden.

Damit es beim Sichern und Wiederherstellen nicht zu Problemen kommt, sollten die Hardware des primären und des Wiederherstellungs-Servers sowie die SQL-Versionen möglichst übereinstimmen.

Snapshot-Monitor im Dashboard

Mithilfe des Monitors Server-Snapshot im ePolicy Orchestrator-Dashboard können Sie Ihre Snapshots zentral verwalten und überwachen.

Wenn der Monitor der Snapshots nicht in Ihrem Dashboard angezeigt wird, erstellen Sie ein neues Dashboard, und fügen Sie es dem Monitor Wiederherstellung nach Systemausfall hinzu.

Abbildung 24-1 Snapshot-Monitor im Dashboard zur Wiederherstellung nach einem Systemausfall

Mithilfe des Monitors Server-Snapshot können Sie Folgendes durchführen:

- Klicken Sie auf **Snapshot erstellen**, um einen McAfee ePO eines McAfee ePO-Servers manuell zu speichern.
- Klicken Sie auf **Siehe Details der letzten Ausführung**, um die Seite **Server-Task-Protokoll: Details** zu öffnen. Auf dieser Seite werden Informationen und Protokolleinträge zum letzten gespeicherten Snapshot angezeigt.
- Überprüfen Sie neben Zeitpunkt der letzten Ausführung den Zeitpunkt (d. h. Datum und Uhrzeit), zu dem der letzte **Snapshot** in der SQL-Datenbank gespeichert wurde.
- Klicken Sie auf den Link **Wiederherstellung nach Systemausfall**, um die Hilfeseite mit Informationen zur Wiederherstellung nach einem Systemausfall anzuzeigen.

Die Farbe und der Titel des Snapshot-Monitors geben Aufschluss über den Status Ihres letzten Snapshots. Beispiel:

- **Blau, Snapshot wird in Datenbank gespeichert** – Der Snapshot-Prozess wird gerade durchgeführt.
- **Grün, Snapshot in Datenbank gespeichert** – Der Snapshot-Prozess wurde erfolgreich abgeschlossen, und der Snapshot ist auf dem aktuellen Stand.
- **Rot, Fehler bei Snapshot** – Während des Snapshot-Prozesses ist ein Fehler aufgetreten.
- **Grau, Kein Snapshot verfügbar** – Es wurde kein Snapshot für eine Wiederherstellung nach einem Systemausfall gespeichert.
- **Orange, Snapshot veraltet** – An der Konfiguration wurden Änderungen vorgenommen, und es wurde kein neuer Snapshot gespeichert. Der Status Snapshot veraltet wird durch folgende Änderungen ausgelöst:
  - Eine Erweiterung wurde geändert (z. B. aktualisiert, entfernt, gelöscht, durch eine neuere oder ältere Version ersetzt).
  - Der Ordner "Keystore" wurde geändert.
  - Der Ordner "conf" wurde geändert.
  - Die Passphrase für die Wiederherstellung nach einem Systemausfall wurde in den Server-Einstellungen geändert.

Task Server-Snapshot für Wiederherstellung nach Systemausfall

Mit dem Task Server-Snapshot für Wiederherstellung nach Systemausfall können Sie den Plan für den Task zum Erstellen eines Server-Snapshots aktivieren oder deaktivieren.

Der Plan für den Task zum Erstellen eines Server-Snapshots ist bei der Microsoft SQL Server-Datenbank standardmäßig aktiviert, bei der Datenbank von Microsoft SQL Server Express Edition hingegen standardmäßig deaktiviert.

Anforderungen für eine Wiederherstellung nach einem Systemausfall

Für eine Wiederherstellung nach Systemausfall müssen die in der folgenden Tabelle aufgeführten Anforderungen hinsichtlich Hard- und Software sowie der Informationen erfüllt sein.

Anforderung	Beschreibung
Hardware-Anforderungen	
Hardware des primären McAfee ePO-Servers	Die Anforderungen an die Server-Hardware hängen von der Anzahl der verwalteten Systeme ab. So können der McAfee ePO-Server und die SQL Server-Datenbank auf der gleichen oder auf unterschiedlicher Hardware installiert sein. Ausführliche Informationen zu den Hardware-Anforderungen finden Sie im *Installationshandbuch von ePolicy Orchestrator 5.1.0*.
Hardware des McAfee ePO-Wiederherstellungs-Servers	Diese Server-Hardware sollte möglichst identisch mit der Hardware des primären McAfee ePO-Servers sein.
Primärer McAfee ePO-Server	Der primäre Server sollte mit einem kürzlich in der SQL-Datenbank gespeicherten Snapshot ordnungsgemäß laufen.
Primäre SQL-Datenbank	In der primären SQL-Datenbank werden die McAfee ePO-Server-Konfiguration, die Client-Informationen sowie die Datensätze aus dem Snapshot für die Wiederherstellung nach einem Systemausfall gespeichert.
Software-Anforderungen	

Anforderung	Beschreibung
Sicherungsdatei der primären SQL-Datenbank	Eine Sicherungsdatei der primären Datenbank, die auch die Snapshot-Datensätze umfasst, können Sie entweder mithilfe von Microsoft SQL Server Management Studio oder der BACKUP-Befehlszeile (Transact-SQL) erstellen.
Software der SQL-Wiederherstellungs-Datenbank	Die primäre Datenbank mit den Snapshot-Datensätzen können Sie entweder mithilfe von Microsoft SQL Server Management Studio oder der RESTORE-Befehlszeile (Transact-SQL) auf dem SQL-Datenbank-Wiederherstellungs-Server wiederherstellen, um die Konfiguration der primären SQL-Datenbank zu duplizieren.
ePolicy Orchestrator	Mit dieser von der McAfee-Website heruntergeladenen Software wird der McAfee ePO-Wiederherstellungs-Server installiert und konfiguriert.
Erforderliche Informationen	
Passphrase für die Schlüsselspeicherverschlüsselung zur Wiederherstellung nach einem Systemausfall	Diese Passphrase wurde während der Erstinstallation von ePolicy Orchestrator hinzugefügt und entschlüsselt die vertraulichen Informationen, die im Snapshot für die Wiederherstellung nach einem Systemausfall gespeichert sind.
Administratorrechte	Sie müssen Zugriff auf den primären und den Wiederherstellungs-Server sowie auf die SQL-Datenbank (z. B. als "DBOwner" und "DBCreator") haben.
Die letzte bekannte Netzwerkadresse (IP-Adresse, DNS-Name oder NetBIOS-Name) des primären McAfee ePO-Servers	Wenn Sie während der Wiederherstellung des McAfee ePO-Servers eine dieser Einstellungen ändern, müssen Sie sicherstellen, dass McAfee Agent eine Möglichkeit hat, den Server zu finden. Am einfachsten erstellen Sie dazu einen CNAME-Eintrag im DNS, der Anfragen, die an die alte Adresse (IP-Adresse, DNS-Name oder NetBIOS-Name) des primären McAfee ePO-Servers gerichtet sind, auf die neuen Informationen des McAfee ePO-Wiederherstellungs-Server verweist.

Funktionsweise der Wiederherstellung nach einem Systemausfall

Für eine schnelle Neuinstallation von ePolicy Orchestrator müssen in regelmäßigen Abständen Snapshots der ePolicy Orchestrator-Konfiguration erstellt werden. Anschließend muss die Datenbank gesichert und auf einem Wiederherstellungs-Server wiederhergestellt sowie ePolicy Orchestrator mit der Option **Wiederherstellen** neu installiert werden.

Überblick über Snapshots zur Wiederherstellung nach einem Systemausfall und Sicherungen

Mithilfe von Snapshots zur Wiederherstellung nach einem Systemausfall, Sicherungen der SQL-Datenbank und Kopiervorgängen wird ein Duplikat der ePolicy Orchestrator-Datenbank auf einem SQL-Datenbank-Wiederherstellungs-Server erstellt.

In diesem Kapitel erhalten Sie einen Überblick über Snapshots zur Wiederherstellung nach einem Systemausfall, Sicherungen der SQL-Datenbank und Kopiervorgänge. Ausführliche Informationen dazu finden Sie unter:

- *Erstellen eines Snapshots*
- *Sichern und Wiederherstellen von Datenbanken mithilfe von Microsoft SQL Server*

Die folgende Abbildung gibt Ihnen einen Überblick darüber, wie die Wiederherstellung von ePolicy Orchestrator nach einem Systemausfall abläuft und welche Hardware erforderlich ist.

In dieser Abbildung ist die SQL-Datenbank auf dem gleichen Computer wie der McAfee ePO-Server installiert. Der McAfee ePO-Server und die SQL-Datenbank können aber auch auf unterschiedlichen Computern installiert sein.

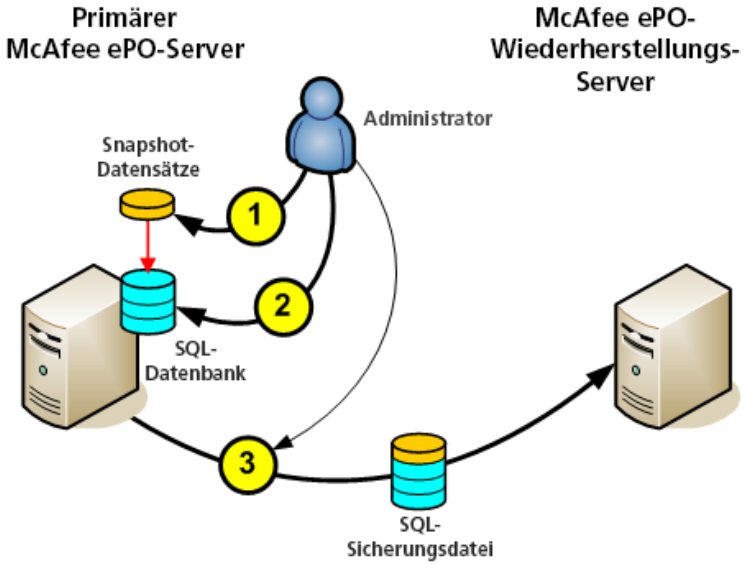


Abbildung 24-2 Snapshot zur Wiederherstellung des McAfee ePO-Servers nach einem Systemausfall und Sicherung

Die Konfiguration der Wiederherstellung von ePolicy Orchestrator nach einem Systemausfall umfasst folgende allgemeine Schritte, die auf dem primären McAfee ePO-Server durchgeführt werden:

1 Erstellen Sie einen Snapshot der McAfee ePO-Server-Konfiguration, und speichern Sie ihn in der primären SQL-Datenbank. Dies kann manuell oder mithilfe eines für diesen Zweck erstellten standardmäßigen Server-Tasks erfolgen.

   In dem erstellten Snapshot werden die folgenden Datenbankdateien gespeichert:

   - C:\Programme\McAfee\ePolicy Orchestrator\Server\extensions – Der Standardpfad zu Informationen über ePolicy Orchestrator-Erweiterungen.
   - C:\Programme\McAfee\ePolicy Orchestrator\Server\conf – Der Standardpfad zu Dateien, die von den ePolicy Orchestrator-Erweiterungen benötigt werden.
   - C:\Programme\McAfee\ePolicy Orchestrator\Server\keystore – Diese Schlüssel sind speziell für die Agent-zu-Server-Kommunikation von ePolicy Orchestrator und die Repositories vorgesehen.

- C:\Programme\McAfee\ePolicy Orchestrator\Server\DB\Keystore – Der Standardpfad zu den Server-Zertifikaten von McAfee-Produktinstallationen.
- C:\Programme\McAfee\ePolicy Orchestrator\Server\DB\Software – Der Standardpfad zu den Installationsdateien von McAfee-Produkten.

  Die gespeicherten Datensätze aus dem Snapshot für die Wiederherstellung nach einem Systemausfall enthalten die Pfade, die Sie für Ihre registrierten ausführbaren Dateien konfiguriert haben. Die registrierten ausführbaren Dateien werden nicht gesichert und müssen von Ihnen beim Wiederherstellen des McAfee ePO-Servers ersetzt werden. Registrierte ausführbare Dateien, deren Pfade nach der Wiederherstellung des McAfee ePO-Servers nicht mehr korrekt sind, werden auf der Seite **Registrierte ausführbare Dateien** rot markiert angezeigt.

Sie sollten die Pfade der registrierten ausführbaren Dateien nach einer Wiederherstellung des McAfee ePO-Servers überprüfen. Auch registrierte ausführbare Dateien, die nicht rot markiert sind, können aufgrund von Abhängigkeitenproblemen Fehler verursachen.

2 Sichern Sie die SQL-Datenbank entweder mithilfe von Microsoft SQL Server Management Studio oder der BACKUP-Befehlszeile (Transact-SQL).

3 Kopieren Sie die in Schritt 2 erstellte Sicherungsdatei für die SQL-Datenbank auf den duplizierten SQL-Wiederherstellungs-Server.

Es ist wichtig, dass Sie die Schritte 2 und 3 abschließen, um die Snapshots vom primären SQL-Server auf den SQL-Wiederherstellungs-Server kopieren und damit die Funktion zur Wiederherstellung nach einem Systemausfall nutzen zu können.

Damit ist die Erstellung und Sicherung des McAfee ePO-Server-Snapshots für Wiederherstellungszwecke nach einem Systemausfall abgeschlossen. Die folgende Wiederherstellungsinstallation des McAfee ePO-Servers müssen Sie nur durchführen, wenn Sie ePolicy Orchestrator neu installieren.

McAfee ePO Überblick über eine Wiederherstellungsinstallation

Die Neuinstallation der Software ePolicy Orchestrator ist der letzte Schritt bei einer schnellen Wiederherstellung des McAfee ePO-Servers.

In diesem Abschnitt erhalten Sie einen Überblick über die Neuinstallation von ePolicy Orchestrator auf dem McAfee ePO-Wiederherstellungs-Server. Ausführliche Informationen finden Sie im *Installationshandbuch*.

Die folgende Abbildung zeigt einen Überblick über die Neuinstallation eines McAfee ePO-Servers.

In dieser Abbildung ist die SQL-Datenbank auf dem gleichen Computer wie der McAfee ePO-Server installiert. Der McAfee ePO-Server und die SQL-Datenbank können aber auch auf unterschiedlichen Computern installiert sein.

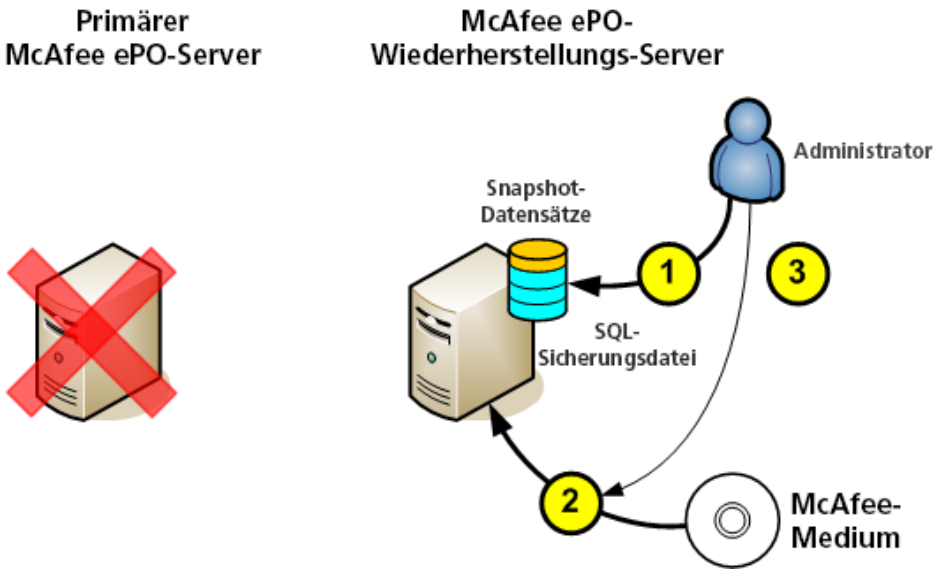


Abbildung 24-3 Wiederherstellungsinstallation eines McAfee ePO-Servers

Bei einer erneuten Installation von ePolicy Orchestrator mithilfe der Snapshot-Datei zur Wiederherstellung nach einem Systemausfall müssen auf dem McAfee ePO-Wiederherstellungs-Server die folgenden allgemeinen Schritte durchgeführt werden:

1 Suchen Sie die Sicherungsdatei der SQL-Datenbank, die Sie im vorherigen Abschnitt in Schritt 3 erstellt haben, und stellen Sie damit die Konfiguration des primären SQL-Servers auf dem SQL-Wiederherstellungs-Server wieder her. Verwenden Sie dabei entweder Microsoft SQL Server Management Studio oder die Methode mit der RESTORE-Befehlszeile (Transact-SQL).

2 Während der Installation der ePolicy Orchestrator-Datenbank-Software:

   a Klicken Sie im Dialogfeld Willkommen auf **ePO aus einem vorhandenen Datenbank-Snapshot wiederherstellen**.

   b Wählen Sie **Microsoft SQL Server** aus, um ePolicy Orchestrator mit der SQL-Wiederherstellungs-Datenbank zu verknüpfen, die die in Schritt 1 wiederhergestellte Konfiguration des primären McAfee ePO-Servers enthält.

   Nachdem die Installation von ePolicy Orchestrator gestartet wurde, werden keine neuen Einträge in der Datenbank erstellt, sondern die Software wird mithilfe der Einträge konfiguriert, die während der Snapshot-Erstellung in der Datenbank gespeichert wurden.

3 Wenn Sie beim Erstellen des McAfee ePO-Wiederherstellungs-Servers die letzten bekannten Informationen (IP-Adresse, DNS-Name oder NetBIOS-Name) des primären McAfee ePO-Servers geändert haben, kann McAfee Agent keine Verbindung zum wiederhergestellten McAfee ePO-Server aufbauen. Am besten erstellen Sie dann einen CNAME-Eintrag im DNS, der Anfragen, die an die Adresse (IP-Adresse, DNS-Name oder NetBIOS-Name) des primären McAfee ePO-Servers gerichtet sind, auf die neuen Informationen des McAfee ePO-Wiederherstellungs-Servers verweist.

Unter *Was ist eine Wiederherstellung nach einem Systemausfall?* finden Sie verschiedene Beispiele für das Wiederherstellen der SQL-Datenbankverbindung zum McAfee ePO-Server.

Nun wird der McAfee ePO-Wiederherstellungs-Server mit exakt der gleichen Konfiguration wie der primäre Server ausgeführt. Die Clients können Verbindungen zum Wiederherstellungs-Server aufbauen, und Sie können diese Clients genau wie vor dem Entfernen des primären McAfee ePO-Servers verwalten.

Erstellen eines Snapshots

Regelmäßige Snapshots Ihres primären McAfee ePO-Servers zur Wiederherstellung nach einem Systemausfall sind der erste Schritt, um einen McAfee ePO-Server schnell wiederherstellen zu können.

Wenn Sie größere Änderungen an der Konfiguration der McAfee-Software vorgenommen haben, sollten Sie mithilfe einer der folgenden Methoden manuell einen Snapshot für die Wiederherstellung nach einem Systemausfall erstellen.

Erstellen Sie zur Automatisierung von Server-Snapshots einen Task "Server-Snapshot für Wiederherstellung nach Systemausfall".

Aufgaben

- *Erstellen von Snapshots im Dashboard* auf Seite 321
  Im ePolicy Orchestrator-Dashboard können Sie mit der Option Snapshot für Wiederherstellung nach Systemausfall Snapshots des primären McAfee ePO-Servers erstellen und den Snapshot-Prozess anhand der Statusänderungen im Dashboard überwachen.
- *Erstellen von Snapshots per Web-API* auf Seite 322
  Über die Web-API von ePolicy Orchestrator können Sie für eine eventuelle Wiederherstellung nach einem Systemausfall Snapshots Ihres primären McAfee ePO-Servers erstellen. Bei dieser Methode können Sie den gesamten Vorgang mit einer einzigen Befehlszeile durchführen.

Erstellen von Snapshots im Dashboard

Im ePolicy Orchestrator-Dashboard können Sie mit der Option Snapshot für Wiederherstellung nach Systemausfall Snapshots des primären McAfee ePO-Servers erstellen und den Snapshot-Prozess anhand der Statusänderungen im Dashboard überwachen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Berichterstellung** | **Dashboards**, um den Monitor **ePO-Server-Snapshot** anzuzeigen.

Falls erforderlich, klicken Sie auf **Monitor hinzufügen**, wählen in der Liste den Monitor **ePO-Server-Snapshot** aus und ziehen ihn in das Dashboard.

2 Klicken Sie auf **Snapshot erstellen**, um mit dem Speichern der McAfee ePO-Server-Konfiguration zu beginnen.

Während der Snapshot-Erstellung wird der Status des Vorgangs in der Titelleiste des **Snapshot-Monitors** angezeigt. Unter *Snapshot-Monitor im Dashboard* finden Sie Informationen zu den Statusanzeigen des Snapshot-Monitors.

Je nach der Komplexität und Größe des von ePolicy Orchestrator verwalteten Netzwerks kann die Snapshot-Erstellung zwischen zehn Minuten und mehr als einer Stunde in Anspruch nehmen. Die Leistung des McAfee ePO-Servers sollte dabei nicht beeinträchtigt werden.

3 Klicken Sie bei Bedarf auf **Siehe Details der aktuellen Ausführung**, um die **Server-Task-Protokolldetails** zum letzten gespeicherten Snapshot anzuzeigen.

> Nach Abschluss der Snapshot-Erstellung klicken Sie auf **Siehe Details der aktuellen Ausführung**, um die **Server-Task-Protokolldetails** zum letzten gespeicherten Snapshot anzuzeigen.

Der aktuelle Snapshot für Wiederherstellung nach Systemausfall wird in der primären SQL-Datenbank des McAfee ePO-Servers gespeichert. Nun kann die Datenbank gesichert und auf den SQL-Datenbank-Wiederherstellungs-Server kopiert werden.

Erstellen von Snapshots per Web-API

Über die Web-API von ePolicy Orchestrator können Sie für eine eventuelle Wiederherstellung nach einem Systemausfall Snapshots Ihres primären McAfee ePO-Servers erstellen. Bei dieser Methode können Sie den gesamten Vorgang mit einer einzigen Befehlszeile durchführen.

Alle in diesem Schritt beschriebenen Befehle werden in die Adresszeile Ihres Web-Browsers eingegeben, um remote auf den McAfee ePO-Server zuzugreifen.

> Bevor das Ergebnis angezeigt wird, werden Sie zur Eingabe des Adminstratorbenutzernamens und -kennworts aufgefordert.

Ausführliche Informationen über die Nutzung der Web-API und entsprechende Beispiele finden Sie im *Skripthandbuch zu McAfee ePolicy Orchestrator 5.1.0*.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Mit dem folgenden Hilfebefehl der ePolicy Orchestrator-Web-API können Sie die zum Ausführen des Snapshots erforderlichen Parameter ermitteln:

`https://localhost:8443/remote/core.help?command=scheduler.runServerTask`

Dabei ist:

- `localhost`: Der Name des McAfee ePO-Servers.
- `8443` – Der Zielport, hier als "8443" (Standardwert) angegeben.
- `/remote/core.help?command=` – Ruft die Web-API-Hilfe auf.
- `scheduler.runServerTask` – Ruft die spezielle Server-Task-Hilfe auf.

> Beim Befehl `runServerTask` muss die Groß- und Kleinschreibung berücksichtigt werden.

Der oben aufgeführte Befehl gibt den folgenden Hilfetext zurück.

```
OK:
scheduler.runServerTask taskName
Führt einen Server-Task aus und gibt anschließend die Task-Protokoll-ID zurück. Mithilfe
der Task-Protokoll-ID können Sie mit dem Befehl
"tasklog.listTaskHistory" den Status des ausgeführten Tasks anzeigen. Gibt die
Task-Protokoll-ID zurück oder löst einen Fehler aus.
Hierfür ist die Berechtigung zum Ausführen von Server-Tasks erforderlich.
Parameter: [taskName (param 1) | taskId]: Eindeutige ID oder eindeutiger Task-Name
```

2 Mit dem folgenden Befehl können Sie alle Server-Tasks auflisten und den taskName-Parameter ermitteln, der zum Ausführen des Tasks zum Erstellen eines Server-Snapshots erforderlich ist:

`https://localhost:8443/remote/scheduler.listAllServerTasks?:output=terse`

Der oben aufgeführte Befehl gibt eine Liste zurück, die in etwa wie folgt aussieht. Wie die Liste im Einzelnen aussieht, hängt von Ihren Berechtigungen und den installierten Erweiterungen ab.

```
OK:
ID Name                                                                    Next Run
-- ------------------------------------------------------------------------ -----------------
14 Update Master Repository                                                8/1/12 at 2:17 AM
7  Synchronize Shared Tasks                                                None
6  Synchronize Shared Policies                                             None
11 RSD: Update Sensor Deployment Client Tasks                              None
10 RSD: Default Delete Detected Systems Task                               None
12 Roll Up Data (Local ePO Server)                                         None
8  Purge Threat and Client Events Older than 90 Days                       None
3  Issue synchronization                                                   None
15 Inactive Agent Cleanup Task                                             None
13 Generate Records for McAfee Agent Compliance History Reporting          None
4  Duplicate Agent GUID - remove systems with potentially duplicated GUIDs None
5  Duplicate Agent GUID - clear error count                                None
9  Download Software Product List                                          8/1/12 at 2:09 AM
2  Disaster Recovery Snapshot Server                                       8/1/12 at 1:59 AM
```

3 Führen Sie mit dem folgenden Befehl den Task zum Erstellen eines Server-Snapshots aus. Verwenden Sie dabei den im vorherigen Schritt ermittelten Task-Namen (`Disaster Recovery Snapshot Server`).

`https://localhost:8443/remote/scheduler.runServerTask?taskName=Disaster%20Recovery%20Snapshot%20Server`

Wenn der Task erfolgreich abgeschlossen wird, sieht die Ausgabe wie folgt aus:

```
OK: 102
```

Je nach der Komplexität und Größe des von ePolicy Orchestrator verwalteten Netzwerks kann die Snapshot-Erstellung zwischen 10 Minuten und bis zu mehr als einer Stunde in Anspruch nehmen. Die Leistung des McAfee ePO-Servers sollte dabei nicht beeinträchtigt werden.

4 Überprüfen Sie, ob der Web-API-Server-Task zum Erstellen des Snapshots erfolgreich ausgeführt wurde.

a Mit dem folgenden Befehl können Sie die ID des Tasks Server-Snapshot für Wiederherstellung nach Systemausfall aus dem Protokoll ermitteln:

`https://localhost:8443/remote/tasklog.listTaskHistory?taskName=Disaster%20Recovery%20Snapshot%20Server`

Dieser Befehl zeigt alle Tasks vom Typ "Server-Snapshot für Wiederherstellung nach Systemausfall" an. Suchen Sie den aktuellsten Task, und notieren Sie sich dessen ID-Nummer. Im Beispiel unten ist das "ID: 102".

```
ID: 102
Name: Server-Snapshot für Wiederherstellung nach Systemausfall
Startdatum: 8/7/12 11:00:34 AM
Enddatum: 8/7/12 11:01:18 AM
Benutzername: admin
Status: Abgeschlossen
Quelle: Planer
Dauer: Weniger als eine Minute
```

b Verwenden Sie den folgenden Befehl mit dieser Task-ID-Nummer 102, um alle zugehörigen Meldungen aus dem Task-Protokoll anzuzeigen.

```
https://localhost:8443/remote/tasklog.listMessages?taskLogId=102
```

Gehen Sie die Meldungen bis zum Ende durch, und suchen Sie nach dem folgenden Eintrag:

```
OK:
Datum: 8/7/12 11:00:34 AM
Meldung: Server-Snapshot erstellen und in Datenbank speichern

Datum: 8/7/12 11:00:34 AM
Meldung: Speicherung des Server-Snapshots in der Datenbank wird gestartet...

. . .

Datum: 8/7/12 11:01:18 AM
Meldung: Server-Snapshot wurde erfolgreich in der Datenbank gespeichert

Datum: 8/7/12 11:01:18 AM
Meldung: Server-Snapshot erstellen und in Datenbank speichern
```

Konfigurieren von Server-Einstellungen zur Wiederherstellung nach einem Systemausfall

Sie können die bei der Installation von ePolicy Orchestrator verwendete Passphrase für die Schlüsselspeicherverschlüsselung ändern und mit einer SQL-Datenbank verknüpfen, die mit Datensätzen aus dem Snapshot für die Wiederherstellung nach einem Systemausfall wiederhergestellt wurde.

Bevor Sie beginnen

Zum Ändern der Passphrase für die Schlüsselspeicherverschlüsselung sind Administratorrechte erforderlich.

Wenn Sie einen McAfee ePO-Server-Snapshot mithilfe der Wiederherstellungsfunktion nach einem Systemausfall erstellen, können Sie den McAfee ePO-Server schnell wiederherstellen.

Für Administratoren ist diese Einstellung nützlich, falls sie die während der Installation von ePolicy Orchestrator konfigurierte Passphrase für die Schlüsselspeicherverschlüsselung vergessen oder verlegt haben. Sie können die zuvor konfigurierte Passphrase ändern, ohne diese kennen zu müssen.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste **Einstellungskategorien** den Eintrag **Wiederherstellung nach Systemausfall** aus, und klicken Sie dann auf **Bearbeiten**.

2 Klicken Sie bei **Passphrase für die Schlüsselspeicherverschlüsselung** auf **Passphrase ändern**. Geben Sie dann die neue Passphrase ein, und bestätigen Sie sie.

Mit der Passphrase für die Schlüsselspeicherverschlüsselung werden im Server-Snapshot gespeicherte vertrauliche Informationen ver- und entschlüsselt. Sie wird während der Wiederherstellung eines McAfee ePO-Servers benötigt. Notieren Sie sich diese Passphrase.

Die ePolicy Orchestrator-Datenbank muss in regelmäßigen Abständen auf einen Wiederherstellungs-Server der Microsoft SQL-Datenbank kopiert werden, um eine aktuelle Sicherung der Datenbank zu erstellen. Informationen zur Vorgehensweise beim Sichern und Wiederherstellen eines Datenbank-Servers finden Sie unter *Konfigurieren eines Snapshots und einer SQL-Datenbank für Wiederherstellungszwecke*.

A Ports – Übersicht

Orientieren Sie sich an diesen Portrichtlinien, wenn Sie die vom McAfee ePO-Server verwendeten Ports anpassen müssen.

Inhalt

- *Ändern des Konsolen-Ports zur Anwendungs-Server-Kommunikation*
- *Ändern des Ports für Agent-Server-Kommunikation*
- *Erforderliche Ports für die Kommunikation durch eine Firewall*
- *Datenverkehr – Kurzanleitung*

Ändern des Konsolen-Ports zur Anwendungs-Server-Kommunikation

Wenn der McAfee ePO-Konsolen-Port zur Anwendungs-Server-Kommunikation von einer anderen Anwendung verwendet wird, führen Sie die folgenden Schritte aus, um einen anderen Port festzulegen.

Bevor Sie beginnen

Dieses Thema enthält Informationen zum Öffnen oder Ändern der Registrierung. Diese Informationen sind nur für Netzwerk- und Systemadministratoren gedacht.

- Es wird dringend empfohlen, die Registrierung zu sichern. Außerdem sollten Sie mit dem Wiederherstellungsprozess vertraut sein. Weitere Informationen finden Sie in der Dokumentation von Microsoft.
- Achten Sie darauf, nur `REG`-Dateien auszuführen, die als echte Registrierungsimportdateien bestätigt sind.

Änderungen an der Registrierung können nicht rückgängig gemacht werden, und fehlerhafte Änderungen können zu Systemfehlern führen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Halten Sie die McAfee ePO-Dienste an:

   a Schließen Sie alle McAfee ePO-Konsolen.

   b Klicken Sie auf **Start** | **Ausführen**, geben Sie `services.msc` ein, und klicken Sie dann auf **OK**.

c Klicken Sie mit der rechten Maustaste auf jeden der folgenden Dienste, und wählen Sie **Anhalten** aus:

- **McAfee ePolicy Orchestrator-Anwendungs-Server**
- **McAfee ePolicy Orchestrator-Ereignisanalyse**
- **McAfee ePolicy Orchestrator-Server**

2 Wählen Sie im Registrierungs-Editor den folgenden Schlüssel aus:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall
\{53B73DFD-AFBE-4715-88A1-777FE404B6AF}]
```

3 Doppelklicken Sie im rechten Bereich auf **TomcatSecurePort.sql**, und ändern Sie die Daten für den Wert in die erforderliche Portnummer (der Standardwert lautet 8443).

4 Öffnen Sie einen Text-Editor, und fügen Sie die folgende Zeile in ein leeres Dokument ein:

```
UPDATE EPOServerInfo SET rmdSecureHttpPort =8443
```

Ändern Sie **8443** in die neue Portnummer.

5 Geben Sie der Datei den Namen `TomcatSecurePort.sql`, und speichern Sie sie an einem temporären Speicherort auf dem SQL-Server.

6 Verwenden Sie Microsoft SQL Server Management Studio, um die erstellte Datei `TomcatSecurePort.sql` zu installieren.

a Klicken Sie auf **Start** | **Alle Programme** | **Microsoft SQL Server Management Studio**.

b Klicken Sie im Dialogfeld Verbindung mit Server herstellen auf **Verbinden**.

c Erweitern Sie **Datenbanken**, und wählen Sie dann **ePO-Datenbank** aus.

d Wählen Sie in der Symbolleiste die Option **Neue Abfrage** aus.

e Klicken Sie auf **Datei** | **Öffnen** | **Datei...**, und suchen Sie dann die Datei TomcatSecurePort.sql.

f Wählen Sie die Datei aus, und klicken Sie auf **Öffnen** | **Ausführen**.

7 Wechseln Sie in Windows-Explorer zu dem folgenden Verzeichnis:

\Programme (x86)\McAfee\ePolicy Orchestrator\Server\conf\

8 Öffnen Sie in Editor die Datei `Server.xml`, und ersetzen Sie alle Einträge für Port 8443 durch die neue Portnummer.

9 Klicken Sie auf **Start** | **Ausführen**, geben Sie `services.msc` ein, und klicken Sie dann auf **OK**.

10 Klicken Sie mit der rechten Maustaste auf jeden der folgenden Dienste, und wählen Sie **Starten** aus:

- **McAfee ePolicy Orchestrator-Anwendungs-Server**
- **McAfee ePolicy Orchestrator-Ereignisanalyse**
- **McAfee ePolicy Orchestrator-Server**

Ändern des Ports für Agent-Server-Kommunikation

Führen Sie die folgenden Schritte aus, um den Port für die Agent-Server-Kommunikation zu ändern.

Bevor Sie beginnen

Dieses Thema enthält Informationen zum Öffnen oder Ändern der Registrierung. Diese Informationen sind nur für Netzwerk- und Systemadministratoren gedacht.

- Es wird dringend empfohlen, die Registrierung zu sichern. Außerdem sollten Sie mit dem Wiederherstellungsprozess vertraut sein. Weitere Informationen finden Sie in der Dokumentation von Microsoft.
- Achten Sie darauf, nur REG-Dateien auszuführen, die als echte Registrierungsimportdateien bestätigt sind.

Änderungen an der Registrierung können nicht rückgängig gemacht werden, und fehlerhafte Änderungen können zu Systemfehlern führen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Halten Sie die McAfee ePO-Dienste an:

   a Schließen Sie alle McAfee ePO-Konsolen.

   b Klicken Sie auf **Start** | **Ausführen**, geben Sie `services.msc` ein, und klicken Sie dann auf **OK**.

   c Klicken Sie mit der rechten Maustaste auf jeden der folgenden Dienste, und wählen Sie **Anhalten** aus:

   - **McAfee ePolicy Orchestrator-Anwendungs-Server**
   - **McAfee ePolicy Orchestrator-Ereignisanalyse**
   - **McAfee ePolicy Orchestrator-Server**

2 Ändern Sie den Wert für den Port in der Registrierung:

   a Klicken Sie auf **Start** | **Ausführen**, geben Sie `regedit` ein, und klicken Sie dann auf **OK**.

   b Navigieren Sie zum entsprechenden Schlüssel für McAfee ePO 5.3.0:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{ 53B73DFD-AFBE-4715-88A1-777FE404B6AF}]

3 Ändern Sie den Zeichenfolgenwert `AgentPort` in den entsprechenden Port. Schließen Sie dann den Registrierungs-Editor. Der Standardwert für diesen Port lautet `80`.

4 Ändern Sie den Wert in der McAfee ePO-Datenbank:

   a Öffnen Sie einen Text-Editor, und fügen Sie die folgenden Zeilen in dem leeren Dokument hinzu:

```
UPDATE EPOServerInfo SET
```

```
ServerHTTPPort=80
```

   b Speichern Sie die Datei als **DefaultAgentPort.sql** an einem temporären Speicherort auf dem SQL-Server.

   c Klicken Sie auf **Start** | **Alle Programme** | **Microsoft SQL Server Management Studio**, um die Datei DefaultAgentPort.sql mithilfe von Microsoft SQL Server Management Studio zu installieren.

d Klicken Sie im Dialogfeld **Verbindung mit Server herstellen** auf **Verbinden**.

e Erweitern Sie **Datenbanken**, und wählen Sie dann **ePO-Datenbank** aus.

f Wählen Sie in der Symbolleiste die Option **Neue Abfrage** aus.

g Klicken Sie auf **Datei** | **Öffnen** | **Datei**, suchen Sie die Datei DefaultAgent.sql, wählen Sie sie aus, und klicken Sie dann auf **Öffnen** | **Ausführen**..

5 Fügen Sie die folgende Zeile in ein leeres Dokument ein:

```
UPDATE EPOServerInfo SET rmdSecureHttpPort =8443
```

Ändern Sie `8443` in die neue Portnummer.

6 Geben Sie der Datei den Namen `TomcatSecurePort.sql`, und speichern Sie sie an einem temporären Speicherort auf dem SQL-Server.

7 Verwenden Sie Microsoft SQL Server Management Studio, um die Datei `TomcatSecurePort.sql` zu installieren.

a Klicken Sie auf **Start** | **Alle Programme** | **Microsoft SQL Server Management Studio**.

b Klicken Sie im Dialogfeld **Verbindung mit Server herstellen** auf **Verbinden**.

c Erweitern Sie **Datenbanken**, und wählen Sie dann **ePO-Datenbank** aus.

d Wählen Sie in der Symbolleiste die Option **Neue Abfrage** aus.

e Klicken Sie auf **Datei** | **Öffnen** | **Datei**, suchen Sie die Datei TomcatSecurePort.sql, wählen Sie sie aus, und klicken Sie dann auf **Öffnen** | **Ausführen**..

8 Ändern Sie den Wert für den Port in den McAfee ePO-Konfigurationsdateien:

a Navigieren Sie zu `C:\Programme (x86)\McAfee\ePolicy Orchestrator\DB\....`

b Öffnen Sie die Datei Server.ini in einem Text-Editor, und ändern Sie den Wert für `HTTPPort=80` in die neue Nummer. Speichern Sie dann die Datei.

c Öffnen Sie die Datei Siteinfo.ini in einem Text-Editor, und ändern Sie den Wert für `HTTPPort=80` in die neue Nummer. Speichern Sie dann die Datei.

d Navigieren Sie zu `C:\Programme (x86)\McAfee\ePolicy Orchestrator\Apache2\conf\...`, öffnen Sie httpd.conf, und ändern Sie die folgenden Zeilen gemäß der neuen Portnummer:

```
Listen 80
```

```
ServerName<NameIhresServers>: 80
```

9 Wenn Sie VirtualHosts verwenden, ändern Sie Folgendes:

```
NameVirtualHost *:80
```

```
<VirtualHost *:80>
```

10 Speichern Sie die Datei, und beenden Sie den Text-Editor.

11 Starten Sie die McAfee ePO-Dienste neu:

a Klicken Sie auf **Start** | **Ausführen**, geben Sie `services.msc` ein, und klicken Sie auf **OK**.

b Klicken Sie mit der rechten Maustaste auf jeden der folgenden Dienste, und wählen Sie **Anhalten** aus:

- **McAfee ePolicy Orchestrator-Ereignisanalyse**
- **McAfee ePolicy Orchestrator-Server**

12 (Optional) Ändern Sie die Einstellungen auf Remote-Agenten-Handlern:

a Vergewissern Sie sich, dass alle McAfee ePO-Konsolen geschlossen sind. Klicken Sie dann auf **Start** | **Ausführen**, geben Sie `services.msc` ein, und klicken Sie auf **OK**.

b Klicken Sie mit der rechten Maustaste auf jeden der folgenden Dienste, und wählen Sie **Anhalten** aus:

- **McAfee ePolicy Orchestrator-Ereignisanalyse**
- **McAfee ePolicy Orchestrator-Server**

Dieser Server wird möglicherweise als MCAFEEAPACHESRV aufgeführt, wenn der Server seit der Installation des Agenten-Handlers nicht neu gestartet wurde.

13 Navigieren Sie zu **C:\Programme (x86)\McAfee\ePolicy Orchestrator\Apache2\conf\...**, öffnen Sie **httpd.conf** in einem Text-Editor, und ändern Sie die folgenden Zeilen gemäß der neuen Portnummer:

```
Listen 80
```

```
ServerName<NameIhresServers>: 80
```

Wenn Sie VirtualHosts verwenden, ändern Sie Folgendes:

```
NameVirtualHost *:80
```

```
<VirtualHost *:80>
```

14 Speichern Sie die Datei, und beenden Sie den Text-Editor.

15 Klicken Sie auf **Start** | **Ausführen**, geben Sie `services.msc` ein, und klicken Sie dann auf **OK**.

16 Klicken Sie mit der rechten Maustaste auf jeden der folgenden Dienste, und wählen Sie **Anhalten** aus.

- **McAfee ePolicy Orchestrator-Ereignisanalyse**
- **McAfee ePolicy Orchestrator-Server**

Dieser Server wird möglicherweise als MCAFEEAPACHESRV aufgeführt, wenn der Server seit der Installation des Agenten-Handlers nicht neu gestartet wurde.

Wenn Sie bereits Agenten auf Clients bereitgestellt haben, installieren Sie den Agenten auf allen Clients neu. Verwenden Sie dabei den Switch /forceinstall, um die vorhandene Datei Sitelist.xml zu überschreiben. Weitere Informationen zu den einzelnen McAfee Agent-Versionen, in denen der Switch /forceinstall verwendet werden kann, finden Sie im McAfee-KnowledgeBase-Artikel KB60555.

Erforderliche Ports für die Kommunikation durch eine Firewall

Verwenden Sie diese Ports, um eine Firewall so zu konfigurieren, dass Datenverkehr zum und vom McAfee ePO-Server zugelassen wird.

Relevante Begriffe

- *Bidirektional*: Die Verbindung kann aus beiden Richtungen initiiert werden.
- *Eingehend*: Die Verbindung wird durch ein Remote-System initiiert.
- *Ausgehend*: Die Verbindung wird durch ein lokales System initiiert.

Tabelle A-1 McAfee ePO-Server

Port	Standard	Beschreibung	Richtung des Datenverkehrs
Port für Agent-Server-Kommunikation	80	Dieser TCP-Port wird vom McAfee ePO-Server-Dienst geöffnet, um Anfragen von Agenten zu empfangen.	Bidirektional zwischen dem Agenten-Handler und dem McAfee ePO-Server und eingehend von McAfee Agent zu Agenten-Handlern und zum McAfee ePO-Server
Über SSL kommunizierender Agent (nur Agenten ab Version 4.5)	443	Standardmäßig muss die Kommunikation von Agenten der Version 4.5 über SSL erfolgen (standardmäßig 443). Dieser Port wird auch vom Remote-Agenten-Handler für die Kommunikation mit dem McAfee ePO-Master-Repository verwendet.	Eingehende Verbindung zum Master-Repository auf dem McAfee ePO-Server von Agenten oder Agenten-Handlern Eingehende Verbindung: • Agent zu McAfee ePO • Agenten-Handler zu Master-Repository • McAfee ePO zu Master-Repository • Agent zu Agenten-Handler
Kommunikationsport für Agentenreaktivierung, SuperAgent-Repository-Port	8081	Dieser TCP-Port wird von Agenten geöffnet, um Agentenreaktivierungsanfragen vom McAfee ePO-Server zu empfangen. Dieser TCP-Port wird geöffnet, um Repository-Inhalte an ein SuperAgent-Repository zu replizieren.	Ausgehende Verbindung vom McAfee ePO-Server und Agenten-Handler zu McAfee Agent
Kommunikationsport für Agentenübertragung	8082	Dieser UDP-Port wird vom SuperAgent geöffnet, um Nachrichten vom McAfee ePO-Server und Agenten-Handler weiterzuleiten.	Ausgehende Verbindung vom SuperAgent zu anderen Agenten
Konsolen-Port zur Anwendungs-Server-Kommunikation	8443	Dieser HTTPS-Port wird vom McAfee ePO-Anwendungs-Server-Dienst geöffnet, um den Zugriff auf die Konsole über einen Web-Browser zuzulassen.	Eingehende Verbindung zum McAfee ePO-Server von der McAfee ePO-Konsole

Tabelle A-1 McAfee ePO-Server *(Fortsetzung)*

Port	Standard	Beschreibung	Richtung des Datenverkehrs
Port für authentifizierte Client-Server-Kommunikation	8444	Wird vom Agenten-Handler verwendet, um mit dem McAfee ePO-Server zu kommunizieren und erforderliche Informationen abzurufen (beispielsweise LDAP-Server).	Ausgehende Verbindung von Remote-Agenten-Handlern zum McAfee ePO-Server
TCP-Port für SQL-Server	1433	Dieser TCP-Port wird für die Kommunikation mit dem SQL-Server verwendet. Dieser Port wird beim Setup automatisch festgelegt oder ermittelt.	Ausgehende Verbindung vom McAfee ePO-Server und Agenten-Handler zum SQL-Server
UDP- Port für SQL-Server	1434	Dieser UDP-Port wird verwendet, um den TCP-Port anzufragen, der von der SQL-Instanz mit der McAfee ePO-Datenbank verwendet wird.	Ausgehende Verbindung vom McAfee ePO-Server und Agenten-Handler zum SQL-Server
Standardmäßiger LDAP-Server-Port	389	LDAP-Verbindung zum Suchen von Computern, Benutzern, Gruppen und Organisationseinheiten für benutzerbasierte Richtlinien	Ausgehende Verbindung vom McAfee ePO-Server und Agenten-Handler zu einem LDAP-Server
Standardmäßiger SSL-LDAP-Server-Port	636	Bei der Funktion Benutzerbasierte Richtlinien wird die LDAP-Verbindung zum Suchen von Benutzern, Gruppen und Organisationseinheiten verwendet.	Ausgehende Verbindung vom McAfee ePO-Server und Agenten-Handler zu einem LDAP-Server

Datenverkehr – Kurzanleitung

Mithilfe dieser Informationen zu Ports und zur Richtung des Datenverkehrs können Sie eine Firewall so konfigurieren, dass Datenverkehr zum und vom McAfee ePO-Server zugelassen wird.

Relevante Begriffe

- *Bidirektional*: Die Verbindung kann aus beiden Richtungen initiiert werden.
- *Eingehend*: Die Verbindung wird durch ein Remote-System initiiert.
- *Ausgehend*: Die Verbindung wird durch ein lokales System initiiert.

Tabelle A-2 Agenten-Handler

Standardport	Protokoll	Richtung des Datenverkehrs auf McAfee ePO-Server	Richtung des Datenverkehrs auf Agenten-Handler
80	TCP	Bidirektionale Verbindung zum und vom McAfee ePO-Server	Bidirektionale Verbindung zum und vom Agenten-Handler
389	TCP	Ausgehende Verbindung vom McAfee ePO-Server	Ausgehende Verbindung vom Agenten-Handler
443	TCP	Eingehende Verbindung zum McAfee ePO-Server	Eingehende Verbindung zum Agenten-Handler

Tabelle A-2 Agenten-Handler *(Fortsetzung)*

Standardport	Protokoll	Richtung des Datenverkehrs auf McAfee ePO-Server	Richtung des Datenverkehrs auf Agenten-Handler
636	TCP	Ausgehende Verbindung vom McAfee ePO-Server	Ausgehende Verbindung vom Agenten-Handler
1433	TCP	Ausgehende Verbindung vom McAfee ePO-Server	Ausgehende Verbindung vom Agenten-Handler
1434	UDP	Ausgehende Verbindung vom McAfee ePO-Server	Ausgehende Verbindung vom Agenten-Handler
8081	TCP	Ausgehende Verbindung vom McAfee ePO-Server	
8443	TCP	Ausgehende Verbindung vom McAfee ePO-Server	Ausgehende Verbindung vom Agenten-Handler
8444	TCP	Eingehende Verbindung zum McAfee ePO-Server	Ausgehende Verbindung vom Agenten-Handler

Tabelle A-3 McAfee Agent

Standardport	Protokoll	Richtung des Datenverkehrs
80	TCP	Ausgehende Verbindung zum McAfee ePO-Server und zum Agenten-Handler
443	TCP	Ausgehende Verbindung zum McAfee ePO-Server und zum Agenten-Handler
8081	TCP	Eingehende Verbindung vom McAfee ePO-Server und vom Agenten-Handler Wenn es sich beim Agenten um ein SuperAgent-Repository handelt, kommen die eingehenden Verbindungen von anderen Agenten.
8082	UDP	Eingehende Verbindungen zu Agenten Die eingehende und ausgehende Verbindung kommt von SuperAgent bzw. ist an einen SuperAgent gerichtet.

Tabelle A-4 SQL Server

Standardport	Protokoll	Richtung des Datenverkehrs
1433	TCP	Eingehende Verbindung vom McAfee ePO-Server und vom Agenten-Handler
1434	UDP	Eingehende Verbindung vom McAfee ePO-Server und vom Agenten-Handler

B Öffnen einer remoten Konsolenverbindung

Mithilfe des Namens oder der IP-Adresse Ihres McAfee ePO-Servers und dessen Kommunikationsport können Sie von jedem unterstützten Internetbrowser aus eine Verbindung herstellen und ePolicy Orchestrator konfigurieren.

Bei einer Remote-Verbindung mit ePolicy Orchestrator sind einige Änderungen an der Konfiguration nicht erlaubt. So können Sie zum Beispiel registrierte ausführbare Dateien nicht über eine Remote-Verbindung ausführen.

Zum Konfigurieren einer Remote-Verbindung müssen Sie den Namen oder die IP-Adresse des McAfee ePO-Servers und dessen Kommunikationsport ermitteln. Wenn Sie bei Ihrem physischen McAfee ePO-Server angemeldet sind, beachten Sie beim Öffnen von ePolicy Orchestrator die Adresse, die in Ihrem Browser angezeigt wird. Diese sieht wie folgt aus:

```
https://win-2k8-epo51:8443/core/orionSplashScreen.do
```

Im oben aufgeführten Beispiel haben die einzelnen Bestandteile der URL-Adresse folgende Bedeutung:

- `win-2k8-epo51` – Der Name des McAfee ePO-Servers
- `:8443` – Die Nummer des Konsolen-Ports zur Anwendungs-Server-Kommunikation, der vom ePolicy Orchestrator-Server verwendet wird.

  Falls Sie diese Nummer nicht geändert haben, lautet der Standardport "8443".

Vorgehensweise

1. Öffnen Sie einen beliebigen Internetbrowser, der von ePolicy Orchestrator unterstützt wird. Eine Liste der unterstützten Browser finden Sie im *Installationshandbuch von McAfee ePolicy Orchestrator*.
2. Geben Sie im Browser eine der folgenden Zeilen in die Adressleiste ein, und drücken Sie dann die **EINGABETASTE**:

   ```
   https://<Server-Name>:8443
   ```

   ```
   https://<IP-Adresse_des_Servers>:8443
   ```

   Beispiel: `https://win-2k8-epo51:8443`
3. Melden Sie sich bei ePolicy Orchestrator an. Damit ist die remote Konsolenverbindung hergestellt.

Im *Skripthandbuch zu ePolicy Orchestrator* finden Sie ausführlichere Beispiele zu Befehlen, die Sie über eine Remote Konsolenverbindung ausführen können.

Index

A

Abfragen 97
- Agent 168
- Aktionen für Ergebnisse 270
- Arbeiten mit 272
- Ausführen, vorhanden 275
- Ausschließen von Tags für Systeme mithilfe der Ergebnisse 144
- Benutzerdefiniert, verwalten 273
- Berechtigungen 269
- Berichtsformate 270
- Diagrammtypen 271
- Ergebnisse als Dashboard-Monitore 270
- Ergebnisse in Tabellenform 271
- Ergebnistyp 279
- Erstellen einer Compliance-Abfrage 221
- Export in Berichtsform 270
- Exportieren in andere Formate 278
- Filter 271
- Geplant 275
- Informationen 270
- Konfigurieren 272
- Persönliche Abfragegruppe 276
- Systemliste zu Tag-Gruppen 145
- Unteraktion 275
- Verwenden in einem Server-Task 222
- Wechseln der Gruppe 277
- Zusammengefasste Daten, von mehreren Servern 279

Abfragen-Generator
- Ergebnistypen 271
- Erstellen von benutzerdefinierten Abfragen 269, 273
- Informationen 271

Abruf-Tasks
- Aktualisieren des Master-Repositorys 88
- Erwägungen beim Planen 88
- Server-Task-Protokoll 247

Active Directory
- Anwenden von Berechtigungssätzen 45
- Benutzeranmeldung 43
- Container, Zuordnen zu Systemstrukturgruppen 129
- Implementierungsstrategien 45
- Konfigurieren der Windows-Autorisierung 47
- Nur Systeme, Synchronisierung 118

Active Directory-Synchronisierung
- Gliederung 114
- Jetzt synchronisieren (Aktion) 116
- Löschen von Systemen 116, 117
- Mit der Systemstruktur 129
- Systeme und Struktur 117
- Tasks 116
- Typen 117
- Umgang mit doppelten Einträgen 116

Administratoren
- Berechtigungen 61
- Erstellen von Gruppen 113
- Informationen 61
- Quellsites, konfigurieren 71
- Verwalten von Benutzerkonten 41

Agent
- Antworten und Weiterleiten von Ereignissen 296
- Bereitgestellte Abfragen 168
- Erster Aufruf des Servers 121
- Gruppieren mithilfe von Zuweisungsregeln 105
- Gruppierung 105
- GUID und Speicherort in der Systemstruktur 121
- Konfigurieren von Proxyeinstellungen 74
- Konfigurieren von Richtlinien zum Verwenden von Repositories 76
- Konvertieren in SuperAgent 154
- McAfee Agent, ePolicy Orchestrator-Komponenten 15
- Reaktivierungen 151
- Relay-Funktionalität 158
- Relay-Funktionalität, Aktivieren 159
- Relay-Funktionalität, Deaktivieren 158
- Wartung 149

Agent-zu-Server-Kommunikation
- Systemstruktursortierung 119

Agenten-Handler
- Authentifizierungsmodi 99

Agenten-Server-Kommunikation
- Informationen 149
- Schlüssel für sichere Agenten-Server-Kommunikation (ASSC) 175
- Verwalten 169

Agentensteuerungen
- Funktionsweise 99
- Informationen 99
- Konfigurieren und Verwalten 102

Agentensteuerungen *(Fortsetzung)*
Mehrere 99
Priorität in Sitelist-Datei 101
Skalierbarkeit 28
Verschieben von Agenten 105
Wann nicht zu verwenden? 28
Wann zu verwenden? 28
Zuweisen von Agenten 102
Zuweisungspriorität 106
Aggregation*, Siehe* Benachrichtigungen
Aktivieren der Relay-Funktionalität des Agenten 159
Aktualisieren
Ausbringungs-Tasks 232
Automatisch, per globaler Aktualisierung 198
DAT-Dateien und Scan-Modul 234
Global, Prozess 196
Planen eines Aktualisierungs-Tasks 239
Prozessbeschreibung 234
Aktualisierungen
Ausbringungspakete 234
Client-Tasks 238
Erwägungen bei der Task-Erstellung 238
Für ausgewählte Systeme 163
Manuelles Einchecken 200
Paket-Signaturen und Sicherheit 232
Pakete und Abhängigkeiten 232
Planen eines Aktualisierungs-Tasks 239
Quellsites 65
Aktualisierungen von DAT-Dateien
Aus Quellsites 71
Ausbringung 234
Erwägungen bei der Task-Erstellung 238
Im Master-Repository 68
Manuelles Einchecken 201
Planen eines Tasks 239
Täglicher Task 239
Aktuell (Zweig)
Definition 68
Einchecken von Aktualisierungspaketen 201
Alternative Sites
Informationen 65
Konfigurieren 71
Löschen 73
Vorhandene bearbeiten 72
Wechseln zu Quellsites 72
Anforderungen für den Systemstrukturzugriff 114
Angewendete Richtlinien
Erstellen von Abfragen 220
Anmeldeinformationen
Ändern von Datenbankregistrierungen 96
Für Ausbringung im Cache ablegen 169
Anmeldeinformationen für Agenten-Ausbringung 169
Anmeldenachrichten 43
Antwort-Generator, Assistent 304
Antworten 97, 299
Auslösende Regeln 304
Ereignisweiterleitung 296
Häufig gestellte Fragen 306
Konfigurieren 296, 301, 304
Konfigurieren zum automatischen Erstellen von Problemen 309
Konfigurierung 298
Kontakte 304
Planen 295
SNMP-Server 299, 300
Zuweisen von Berechtigungen 299
Antwortregeln
Beschreibung (Seite) 303
Einrichten von Filtern 303
Erstellen und Bearbeiten 303
Festlegen von Schwellenwerten 304
Anzeigen von Problemdetails 309
ASKI, siehe Agent-zu-Server-Kommunikationsintervall 150
ASSC-Schlüssel, siehe Schlüssel für sichere Agenten-Server-Kommunikation 134
Audit-Protokoll
Anzeigen und Bereinigen des Aktionsverlaufs 48
Automatisches Bereinigen 49
Informationen 48
Verwendet bei Produktausbringung 191
Ausbringung
Anzeigen 191
Anzeigen eines zugewiesenen Client-Tasks 239
Globale Aktualisierung 198
Installieren von Produkten 235, 237
Manuelles Einchecken von Paketen 200
Neues Produkt, Beispiel 195
Paketsicherheit 232
Produkt und Aktualisierung, erstmalig 234
Produkte und Aktualisierungen 234
Tasks 232
Tasks, für verwaltete Systeme 235
Unterstützte Pakete 232
Ausführbare Dateien
Verwalten 301
Ausgewählte Pakete
Deaktivieren der Replizierung 82
Replizierung vermeiden 82
Authentifizierung
Konfigurieren für Windows 46
Authentifizierung, Konfigurieren für Windows 43
Automatische Antworten 163, 293
Autorisierung
Strategien 45

B

Bandbreite
Erwägungen bei Abruf-Tasks 88
Erwägungen bei der Ereignisweiterleitung 302

Bandbreite *(Fortsetzung)*
Replizierungs-Tasks 89
Verteilte Repositories 65
Bearbeiten von Datenbank-Server-Registrierungen 96
Bearbeiten von Problemen 309
Bedrohungsereignisprotokoll
Anzeigen und Bereinigen 254
Informationen 253
Beispiel für VirusScan Enterprise
Ausbringung 195
Benachrichtigungen
Beschränkung, Aggregation und Gruppierung 138, 294
Empfänger 138
Ereignisweiterleitung 297
Funktionsweise 138
Registrierte ausführbare Dateien, verwalten 301
SNMP-Server 94, 300
Zuweisen von Berechtigungen 298
Benachrichtigungsregeln
Importieren von MIB-Dateien 300
Standardabfragen 139, 294
Benutzer
Berechtigungssätze 61
Benutzerbasierte Richtlinien
Informationen 217
Kriterien 217
Benutzerdefinierte Anmeldenachrichten 43
Benutzerkonten
Ändern von Kennwörtern 41
Typen 41
Verwalten 41
Benutzeroberfläche
Menü 20
Berechtigungen
Administrator 61
Für Abfragen 269
Für Dashboards 260
Zuweisen für Antworten 299
Zuweisen für Benachrichtigungen 298
Berechtigungssätze 97
Anwenden auf Active Directory-Gruppen 45
Beispiel 61
Exportieren und Importieren 62
Interaktion mit Benutzern und Gruppen 61
Systemstruktur 114
Verwalten 62
Zuordnen zu Active Directory-Gruppen 43
Zuweisen zu Berichten 288
Bereinigen abgeschlossener Probleme 310
Manuell 310
Bericht-Generator
Erstellen von benutzerdefinierten Berichten 269
Berichte 257
Ändern der Reihenfolge von Elementen 288
Anzeigen von Ergebnissen 288
Berichte 257
Arbeiten mit 282
Ausführen 289
Ausführen mit einem Server-Task 289
Entfernen von Elementen 287
Erstellen 269, 283
Exportieren und Importieren 290
Exportierte Abfrageergebnisse 270
Formate 270
Hinzufügen von Elementen 284
Hinzufügen zu einer Gruppe 288
Informationen 281
Konfigurieren 272
Konfigurieren der Vorlage und des Speicherorts 291
Konfigurieren von Bildelementen 285
Konfigurieren von Diagrammelementen 286
Konfigurieren von Tabellenelementen 286
Konfigurieren von Textelementen 285
Kopf- und Fußzeilen 287
Löschen 292
Planen 289
Struktur und Seitengröße 281
Vorhandene bearbeiten 283
Berichtelemente
Ändern der Reihenfolge 288
Entfernen 287
Konfigurieren von Bildern 285
Konfigurieren von Diagrammen 286
Konfigurieren von Tabellen 286
Konfigurieren von Text 285
Beschränkung*, Siehe* Benachrichtigungen
Betriebssysteme
Ältere Systeme (Windows 95, Windows 98) 115
Filter für Antwortregel 303
Gruppierung 115

C

Client-Tasks
Anzeigen 239
Arbeiten mit 241
Bearbeiten von Einstellungen 242
Client-Task-Katalog 231
Erstellen 241
Freigeben 231
Informationen 231
Löschen 242
Objekte 231
Sofort ausführen 165
Vergleich 243
Verglichen mit Produktausbringungsprojekten 188
Client-Tasks vergleichen 243
Client-Tasks, On Demand 165
Client-Zertifikatauthentifizierung
Aktivieren 51

Client-Zertifikatauthentifizierung *(Fortsetzung)*
Deaktivieren 52
Einführung 50
Fehlerbehebung 54
Konfigurieren von Benutzern 52
Konfigurieren von ePolicy Orchestrator 51
Strategien zur Verwendung 50
Cloud-Verwaltung
Funktionsweise der Software 16
Compliance
Erstellen einer Abfrage 221
Generieren von Ereignissen 222
CRL-Datei, Aktualisierung in "Zertifikatbasierte Authentifizierung" 53

D

Dashboard-Monitore
Konfigurieren 263
Verschieben und Ändern der Größe 265
Dashboards 97
Aktualisierungsintervalle 267
Beschreibungen 265
Einführung 259
Enthaltene Monitore 265
Erste Anmeldung 267
Erstellen, Snapshot 321
Gewähren von Berechtigungen 260
Importieren und Exportieren 262
Konfigurieren für exportierte Berichte 291
Konfigurieren von Monitoren 263
McAfee 259
Öffentlich 259
Privat 259
Server-Einstellungen 267
Standard-Monitore 265
Verschieben und Ändern der Größe von Monitoren 265
Verwalten 260
DAT-Dateien
Siehe auch Virusdefinitionsdateien
Löschen aus Repository 200
Repository-Zweige 201
Testen 240
Datenbank
Wiederherstellen der SQL-Datenbank 250
Datenbank-Server
Bearbeiten von Registrierungen 96
Entfernen 96
Informationen zur Verwendung 95
Registrieren 96
Datenbanken
Abfragen mehrerer Server 279
Abfragen und Abrufen von Daten 270
Planen eines Snapshots 250
Ports und Kommunikation 20
Datenbanken
Sicherungs- und Wiederherstellungsprozess 251
Überblick über Sicherung 317
Überblick über Wiederherstellung 319
Wiederherstellung nach Systemausfall 314
Deaktivieren der Relay-Funktionalität des Agenten 158
Diagramme, siehe Abfragen 271
Dienstprogramme
NETDOM.EXE, Erstellen einer Textdatei 125
Dokumentation
Produktspezifisch, suchen 12
Typografische Konventionen und Symbole 11
Zielgruppe dieses Handbuches 11
Domänensynchronisierung 114
Doppelte Einträge in der Systemstruktur 130

E

E-Mail-Server
Konfigurieren von Antworten 298
Eigenschaften
McAfee Agent, Anzeigen in der Konsole 168
Produkt 166
System 166
Überprüfen von Richtlinienänderungen 168
Einrichten 25
Empfehlungen von McAfee
Ausbringen von Agenten beim Importieren großer Domänen 130
Gliederung für die Organisation, beurteilen 114
Planen der Systemstruktur 114
Planen von Replizierungs-Tasks 89
Richtlinien vor der Zuweisung duplizieren 205
Schrittweise Produktausbringung 232
Server-Task zum Zusammenfassen von Daten erstellen 280
Verwenden globaler Aktualisierung 196
Empfohlene Vorgehensweisen
Agent-Server-Kommunikationsintervall 149
Duplizieren von Richtlinien vor dem Zuweisen 205
Erstellen der Systemstruktur 122
Importieren von Active Directory-Containern 129
Produktausbringung 232
Sperren der Richtlinienzuweisung 205
Entfernen von Datenbank-Server-Registrierungen 96
ePolicy Orchestrator
Anmelden und Abmelden 19
Einführung 13
Funktionsweise der Software 16
Grundlegende Funktionen 35
Informationen 15
Remote Konsolenverbindung 335
Ereignisse
Benachrichtigungsintervalle 302
Bestimmen, welche Ereignisse weitergeleitet werden 302
Compliance-Ereignisse 222
Filtern, Server-Einstellungen 20

Ereignisse *(Fortsetzung)*
Systemliste zu Tag-Gruppen 145
Weiterleiten und Benachrichtigungen 297
Erfassungsgruppen 120
Erstellen von Problemen 308
Erweiterungsdateien
Installieren 199
Erzwingen, siehe Richtlinienerzwingung 212
Exportieren
Abfragen 97
Antworten 97, 299
Berechtigungssätze 62
Berichte 290
Client-Task-Objekte 97
Dashboards 97
Repositories 97
Richtlinien 97
Richtlinienzuweisungen 97
Systeme 97
Tags 97
Tasks 97
Exportieren von Systemen 124

F

Failback auf den ursprünglichen Server 319
Fehlerbehebung
Client-Zertifikatauthentifizierung 54
Produktausbringung 232
Überprüfen der Eigenschaften von McAfee Agent und Produkten 168
Filter
Abfrageergebnisse 271
Einstellung für Antwortregeln 303
Einstellungen der Ereignisfilterung 20
Für Server-Task-Protokoll 247
Liste 23
FTP-Repositories
Aktivieren der Ordnerfreigabe 83
Bearbeiten 83
Erstellen und Konfigurieren 79
Informationen 67
Funktionen, ePolicy Orchestrator
Komponenten 15

G

Generator für Server-Tasks 148
Geographische Gliederung, Vorteile 114
Gliederung, siehe Organisation der Systemstruktur 114
Global Unique Identifier (GUID) 121
Globale Administratoren
Erforderliche Berechtigungen für Wiederherstellung nach Systemausfall 314
Globale Aktualisierung
Aktivieren 198
Anforderungen 196
Globale Aktualisierung
Prozessbeschreibung 196
Globale Aktualisierungen
Inhalte 75
Gruppe Eigenes Unternehmen der Systemstruktur 112
Gruppen
Anzeigen der Richtlinienzuweisung 225
Betriebssysteme und 115
Definieren mithilfe der IP-Adresse 115
Einfügen von Richtlinienzuweisungen 214
Erfassungsgruppe 120
festgelegt 113
Importieren von NT-Domänen 130
Konfigurieren von Kriterien für die Sortierung 127
Kriterienbasiert 121
Manuelle Erstellung 123
Manuelles Aktualisieren mit NT-Domänen 133
Manuelles Verschieben von Systemen 134
Richtlinien, Vererbung von 113
Richtlinienerzwingung für ein Produkt 212
Sortierung, automatisiert 115
Sortierungskriterien 126
Steuern des Zugriffs 61
Gruppierung*, Siehe* Benachrichtigungen

H

Handbuch, Informationen 11
Hierarchie von SuperAgents 156, 157
Hinzufügen von Kommentaren zu Problemen 309
HTTP-Repositories
Aktivieren der Ordnerfreigabe 83
Bearbeiten 83
Erstellen und Konfigurieren 79
Informationen 67

I

Importieren
Abfragen 97
Antworten 97, 299
Berechtigungssätze 62
Berichte 290
Client-Task-Objekte 97
Dashboards 97
Grundlagen 97
Repositories 97
Richtlinien 97
Richtlinienzuweisungen 97
Systeme 97
Tags 97
Tasks 97
Inaktive Agenten 166
Installation
Planen 27

Internet Explorer
Konfigurieren von Proxyeinstellungen 74
Intervall für Benachrichtigungsereignisse 302
Intervalle
Zwischen Benachrichtigungen 302
IP-Adresse
Als Gruppierungskriterien 115
Bereich, als Sortierungskriterien 127
IPv6 28
Sortierung 120
Sortierungskriterien 122, 127
Subnetzmaske, als Sortierungskriterien 127
Überprüfen von IP-Überschneidung 120
IP-Integrität überprüfen (Aktion) 120

J

Jetzt sortieren (Aktion) 118

K

Kennwörter
Ändern in Benutzerkonten 41
Unterstützte Formate 42
Komponenten
ePolicy Orchestrator, Informationen 15
McAfee ePO-Server, Informationen 15
Repositories, Informationen 65
Wiederherstellung nach Systemausfall 314
Konfiguration
Grundlegende Funktionen 34
Systemliste zu Tag-Gruppen 145
Überblick 31
Kontakte
Antworten 304
Konten
Benutzertypen 41
Konventionen und Symbole in diesem Handbuch 11
Konvertieren von Agenten in SuperAgents 154
Kriterienbasierte Tags
Sortierung 127
Übernehmen 147, 148

L

LAN-Verbindungen und geographische Gliederung 114
LDAP-Server
Authentifizierungsstrategien 45
LDAP-Server, registrieren 93
Listen
Filtern 23
Suchen 23
Listen, Arbeiten mit 22
Lizenzschlüssel 38
Lokale verteilte Repositories 85
Löschen von Problemen 309

M

Master-Repositories
Informationen 65
Kommunikation mit Quellsites 73
Konfigurieren von Proxyeinstellungen 73
Verwenden von Replizierungs-Tasks 89
Master-Repository
Aktualisieren mit Abruf-Tasks 88
ePolicy Orchestrator-Komponenten 15
Manuelles Einchecken von Paketen 201
Schlüsselpaar für nicht signierte Inhalte 172
Sicherheitsschlüssel in Umgebungen mit mehreren Servern 174
McAfee Agent
Eigenschaften, anzeigen 168
Statistiken 162
McAfee Agent, siehe Agent 15
McAfee Default (Richtlinie)
Häufig gestellte Fragen 228
McAfee Product Improvement Program
Entfernen des Programms 39
Konfigurieren 38
McAfee ServicePortal, Zugriff 12
McAfee-Empfehlungen
IP-Adresse für die Sortierung verwenden 115
Tag-basierte Sortierungskriterien verwenden 115
McAfee-Links, Standard-Monitor 265
Mehrere McAfee ePO-Server
Richtlinienfreigabe 228
Menü
Navigieren in der Benutzeroberfläche 20
Menübasierte Navigation 19
Microsoft Internetinformationsdienste (IIS) 67
Microsoft Windows Resource Kit 125
Monitore 259
Enthalten in Dashboards 265
Konfigurieren 263
Monitore, Wiederherstellung nach Systemausfall
Snapshot-Status 314
My Default (Richtlinie)
Häufig gestellte Fragen 228

N

Nachricht
Benutzerdefinierte Anmeldung 43
Navigation
Menü 20
Menübasiert 19, 20
Navigationsleiste 20
NETDOM.EXE (Dienstprogramm), Erstellen einer Textdatei 125
Netzwerkbandbreite, siehe Organisation der Systemstruktur 114
Neue Gruppe, Assistent
Erstellen neuer Gruppen 276
Nicht verwaltete Repositories 67

NT-Domänen
Aktualisieren synchronisierter Gruppen 133
Importieren in manuell erstellte Gruppen 130
Synchronisierung 118, 130

O

Oberfläche
Favoritenleiste 19
Menü 19
Navigation 19
Organisation der Systemstruktur
Betriebssysteme 115
Doppelte Einträge 130
Erstellen von Gruppen 122
Erwägungen beim Planen 114
Gliederung im Netzwerk 114
Hinzufügen von Systemen zu Gruppen 124
Importieren von Active Directory-Containern 129
Importieren von Systemen und Gruppen 126
Manuelles Verschieben von Systemen in Gruppen 134
Netzwerkbandbreite 114
Textdateien, Importieren von Systemen und Gruppen 125
Verwenden von Untergruppen 130
Zuordnen von Gruppen zu Active Directory-Containern 129

P

Pakete
Konfigurieren des Ausbringungs-Tasks 237
Manuelles Einchecken 200
Sicherheit 232
Verschieben zwischen Zweigen im Repository 201
Passphrase für die Schlüsselspeicherverschlüsselung
Einstellung 324
Wiederherstellung nach Systemausfall 314
Peer-to-Peer; bewährte Vorgehensweisen 161
Planen
Anwenden von kriterienbasierten Tags 148
Server-Tasks mit Cron-Syntax 246
Snapshot für Wiederherstellung nach Systemausfall 250
Port für Agenten-Kommunikation 170
Ports
Agenten-Kommunikation 170
Server-Einstellungen 20
Server-Einstellungen und Kommunikation 20
Probleme
Ändern 309
Anzeigen von Details 309
Arbeiten mit 307
Automatisches Erstellen aus Antworten 309
Erstellen 308
Hinzufügen von Kommentaren 309
Informationen 307
Löschen 309
Verwalten 307
Probleme
Zuweisen 309
Probleme, bereinigen
Abgeschlossene Probleme 310
Planmäßiges Bereinigen abgeschlossener Probleme 311
Problemverwaltung 307
Product Improvement Program
Entfernen des Programms 39
Konfigurieren 38
Produktaktualisierungen
Ausbringen 234
Manuelles Einchecken von Paketen 200
Paket-Signaturen und Sicherheit 232
Prozessbeschreibung 234
Quellsites und 65
Unterstützte Pakettypen 232
Produktausbringung
Anzeigen 191
Anzeigen eines zugewiesenen Client-Tasks 239
Erstellen 192
Informationen über das Überwachen und Ändern 190
Methoden 187
Überwachen und Ändern 194
Verglichen mit der Client-Task-Ausbringungsmethode 188
Produktausbringungspakete
Aktualisierungen 232
Einchecken 200
Manuelles Einchecken 201
Sicherheit und Paket-Signaturen 232
Unterstützte Pakete 232
Produktbereitstellung
Projekte 188
Produkteigenschaften 166
Produktinstallation
Installieren von Erweiterungsdateien 199
Konfigurieren von Ausbringungs-Tasks 235, 237
Produktkompatibilitätsliste
Konfigurieren der Download-Quelle 185
Überblick 183
Protokolldateien
Server-Task-Protokoll 247
Proxyeinstellungen
Agent 74
Konfigurieren für Master-Repository 73
Server-Einstellungen 38

Q

Quellsites
Aktualisierungspakete 234
Alternative Site 65
Erstellen 71
Importieren aus SITEMGR.XML 88
Informationen 65
Konfigurierung 71

Quellsites *(Fortsetzung)*
Löschen 73
Produktaktualisierungen 65
Vorhandene bearbeiten 72
Wechseln zu alternativen Sites 72

R

Reaktivierungen
An Systemstrukturgruppen 152
Informationen 151
Manuell 151
SuperAgents 151, 153
Tasks 151
Regeln
Einrichten für Benachrichtigungen, SNMP-Server 300
Konfigurieren von Kontakten für Antworten 304
Standards für Benachrichtigungen 139, 294
Registrieren von Datenbank-Servern 96
Registrierte Server
Aktivieren der Richtlinienfreigabe 227
Hinzufügen von SNMP-Servern 94
LDAP-Server, hinzufügen 93
Registrieren 91
Unterstützt von ePolicy Orchestrator 91
Relay-Funktionalität 158
Relay-Funktionalität, Aktivieren 159
Relay-Funktionalität, Deaktivieren 158
Remote Konsolenverbindung 335
Replizierung
Deaktivieren für ausgewählte Pakete 82
Vermeiden für ausgewählte Pakete 82
Replizierungs-Tasks
Aktualisieren des Master-Repositorys 89
Server-Task-Protokoll 247
Vergleich von vollständiger und inkrementeller Replizierung 89
Repositories 97
Anordnen, SuperAgents, Hierarchie 156, 157
Art und Weise ihrer Zusammenarbeit 70
Erstellen eines SuperAgent-Repositorys 77
Importieren aus Repository-Listen-Dateien 88
Konzept 65
Master, Konfigurieren von Proxyeinstellungen 73
Nicht verwaltet, Kopieren von Inhalten 85
Quellsite 65
Replizierung und Auswahl 90
Sicherheitsschlüssel 171, 174
Typen 65
UNC 84
Zweige 68, 201, 240
Repository-Listen-Dateien
Arbeiten mit 86
Exportieren 87
Hinzufügen eines verteilten Repositorys 80
Importieren 88
Repository-Listen-Dateien
Informationen 69
Priorität von Agentensteuerungen 101
SITELIST.XML, Verwendung 69
Richtlinien 97
Ändern des Besitzers 209
Anwenden auf Systeme 205
Anzeigen 203, 223
Arbeiten mit dem Richtlinienkatalog 206
Automatische Antwort 163
Besitz 205, 224
Einstellungen, anzeigen 224
Freigeben zwischen McAfee ePO-Servern 210
Gruppenvererbung, anzeigen 225
Häufig gestellte Fragen 228
Importieren und Exportieren 203, 210, 211
Informationen 203
Kategorien 203
Konfigurieren 208
Reagieren auf Ereignisse 163
Steuern, auf der Seite "Richtlinienkatalog" 206
Überprüfen von Änderungen 168
Unterbrochene Vererbung, zurücksetzen 226
Vererbung 205
Vergleich 226
Verwalten, auf der Seite "Richtlinienkatalog" 207
Zuweisen mithilfe von Tags 218
Zuweisen und Verwalten 208
Richtlinien vergleichen 226
Richtlinienereignisse
Reagieren auf 163
Richtlinienerzwingung
Aktivieren und Deaktivieren 212
Anzeigen von Zuweisungen mit deaktivierter Erzwingung 224
Erzwingen von Richtlinien 203
Für ein Produkt 212, 213
Richtlinienfreigabe
Bestimmen 227
Mehrere McAfee ePO-Server 227
Registrieren des Servers 227
Verwenden eines registrierten Servers 227
Verwenden von Server-Tasks 227, 228
Zuweisen 227
Richtlinienkatalog
Arbeiten mit 206
Seite, anzeigen 203
Richtlinienverwaltung
Arbeiten mit Client-Tasks 241
Erstellen von Abfragen 220
mit Gruppen 113
Richtlinienzuweisung
Anzeigen 223, 225
Deaktivierte Erzwingung, anzeigen 224
Gruppe, zuweisen 211

Richtlinienzuweisung *(Fortsetzung)*
Kopieren und Einfügen 213–215
Richtlinienkatalog 205
Sperren 205
Systeme, zuweisen 211, 212
Richtlinienzuweisungsregeln 216
Anzeigen der Zusammenfassung 219
Bearbeiten der Priorität 219
Benutzerbasiert 216
Benutzerbasierte Richtlinien 217
Erstellen 218
Importieren und Exportieren 219
Informationen 216
Löschen und Bearbeiten 219
Priorität 216
Regelkriterien 216
Richtlinien für mehrere Richtlinienplätze 216
Systembasiert 216
Systembasierte Richtlinien 218

S

Sammelgruppe 112
Scan-Modul-Aktualisierung
Ausbringungspakete 234
Manuelles Einchecken 201
Scan-Modul, aktualisieren
Aus Quellsites 71
Im Master-Repository 68
Planen eines Tasks 239
Scan-Module
Löschen aus Repository 200
Repository-Zweige 201
Schlüssel*, Siehe* Sicherheitsschlüssel
Schlüssel für sichere Agenten-Server-Kommunikation
Exportieren und Importieren von Schlüsseln 136
mit Systeme übertragen 134
Schnelle Systemsuche, Standard-Monitor 265
Schnellsuche 23
Server
Datenbank 95
Einstellungen und Steuern des Verhaltens 20
Freigeben von Objekten zwischen 97
Freigeben von Richtlinien 210
Hardware-Upgrade mit Wiederherstellung nach Systemausfall 313
Importieren und Exportieren von Abfragen 277
Importieren von Richtlinien 211
Konfiguration, Überblick 31
LDAP-Server, registrieren 93
McAfee ePO-Server, Komponenten 15
Registrierbare Typen 91
Registrieren zusätzlicher Server 91
Schlüsselpaar für Master-Repository 172
Sicherungs- und Wiederherstellungsprozess 251
SNMP und Antworten 299
Server
SNMP und Benachrichtigungen 300
Überblick über Sicherung 317
Überblick über Wiederherstellung 319
Übertragen von Systemen 135
Unterstützte Server-Typen 91
Verwenden mehrerer 27
Wiederherstellung nach Systemausfall 252, 314
Server-Einstellungen
Benachrichtigungen 139, 294
Dashboards 20
Globale Aktualisierung 198
Globale Aktualisierungen 75
Internet Explorer 74
Ports und Kommunikation 20
Proxy und Master-Repositories 65
Proxyeinstellungen 38
SSL-Zertifikate 54
Standardkategorien 20
Typen 20
Wiederherstellung nach Systemausfall 324
Server-Task planen
Für Richtlinienfreigabe 228
Server-Task zum Zusammenfassen von Daten 280
Server-Task-Protokoll
Informationen 247
Tasks anzeigen, filtern und bereinigen 247
Server-Tasks
Abfrage mit Unteraktion 275
Ausführen von Berichten 289
Domänen/Active Directory, synchronisieren 116
Ersetzen des Server-Zertifikats 55
Erstellen 245
Für Richtlinienfreigabe 227
Informationen 245
Planen einer Abfrage 275
Planen mit Cron-Syntax 246
Protokolldatei, bereinigen 247
Server-Task-Protokoll 247
Wiederherstellung nach Systemausfall 250
Zulassen von Cron-Syntax 246
Zusammenfassen von Daten 280
Server-Typen
Unterstützt von ePolicy Orchestrator 91
Server-Zertifikat
Entfernen 52
Ersetzen 55
ServicePortal, Quellen für Produktinformationen 12
Sichere Agenten-Server-Kommunikation (ASSC)
Anzeigen von Systemen, die ein Schlüsselpaar verwenden 177
Arbeiten mit Schlüsseln 175
Informationen 171
Mithilfe eines Schlüsselpaares 177
Verwenden verschiedener Schlüsselpaare für Server 178

Sicherheitsschlüssel
Allgemein 171
ASSC, Arbeiten mit 175
Für Inhalte aus anderen Repositories 172
Hauptschlüssel in Umgebungen mit mehreren Servern 174
Mithilfe eines Hauptschlüssels 173
Privat und öffentlich 172
Server-Einstellungen 20
Sichere Agenten-Server-Kommunikation (ASSC) 171, 175
Verwalten 173
Sicherheitsverwaltung 109
Sicherheitszertifikat
Erstellen eines selbstsignierten Zertifikats 57
Installieren 55, 56
Zertifizierungsstelle 54
Sicherungs- und Wiederherstellungsprozess
Für SQL-Datenbank 251
Sitelist-Dateien 101
Sites
Alternative Site 65, 71
Löschen von Quellsites oder alternativen Sites 73
Vorhandene bearbeiten 72
Wechseln zwischen Quellsites und alternativen Sites 72
Skalierbarkeit
Horizontal 27
Informationen 27
Mithilfe mehrerer Server 27
Mithilfe von Agentensteuerungen 28
Planen 27
Vertikal 27
Snapshot
Dashboard-Monitor 314
Erstellen 321
Erstellen im Dashboard 321
Erstellen über Web-API 322
In Datenbank gespeicherte Datensätze 317
Planen von Standardwerten 250
Server-Task-Protokolldetails 321
Teil der Wiederherstellungen nach Systemausfall 313
Überblick 317
Snapshots
Konfigurieren 250
SNMP-Server
Siehe auch Antworten

Registrieren 94
Software-Manager 181
Einchecken von Erweiterungen 182
Einchecken von Paketen 182
Entfernen von Erweiterungen 182
Entfernen von Paketen 182
Informationen 181
Inhalte 181
Lizenzierte Software 182
Produktkompatibilität 183
Software-Manager 181
Test-Software 182
Sortiertest (Aktion) 118
Sortierungskriterien
Auf IP-Adressen basierend 127
Für Gruppen 127
Gruppen, automatisiert 115
IP-Adresse 120
Konfigurierung 127
Sortieren von Systemen in Gruppen 118
Tag-basiert 115, 120, 127
SPIPE 149
Sprachpakete, siehe Agent 114
SQL Server*, Siehe* Datenbanken
SQL-Datenbank
Planen eines Snapshots 250
Sicherungs- und Wiederherstellungsprozess 251
Überblick über Sicherung 317
Überblick über Wiederherstellung 319
Wiederherstellen der Datenbank 250
Wiederherstellung nach Systemausfall 314
SSL-Zertifikate
Informationen 54
Steuerungen
Erstellen von Gruppen 104
Gruppieren von Agenten 107
Priorität 101
Verschieben von Agenten 105
Steuerungsgruppen
Bearbeiten von Einstellungen 104
Erstellen 104
Informationen 101
Löschen 104
Steuerungszuweisung
Anzeigen der Zusammenfassung 103
Bearbeiten der Priorität 103, 106
Verwalten 103
Subnetze, als Gruppierungskriterien 115
SuperAgent-Repositories
Anforderungen für globale Aktualisierungen 196
Erstellen 77
Informationen 67
Löschen 78
Replizieren von Paketen 78
Tasks 77
SuperAgents
Agenten konvertieren 154
Caching 155
Hierarchie 156, 157
Informationen zu 153
Reaktivierungen 151, 153
Reaktivierungen an Systemstrukturgruppen 152
Verteilte Repositories 67
Synchronisierung
Active Directory und 118

Synchronisierung *(Fortsetzung)*
Ausschließen von Active Directory-Containern 117
Automatisches Ausbringen von Agenten 117
Jetzt synchronisieren (Aktion) 116
NT-Domänen 118
Nur Systeme, mit Active Directory 118
Planen 132
Standard 121
Systeme und Strukturen 117
Verhindern doppelter Einträge 118
Systembasierte Richtlinien
Informationen 218
Kriterien 218
Systeme 97
Anzeigen der Richtlinienzuweisung 225
Eigenschaften 166
Einfügen von Richtlinienzuweisungen 215
Exportieren aus der Systemstruktur 124
Richtlinienerzwingung für ein Produkt 213
Sortieren in Gruppen 128
Zuweisen von Richtlinien 211, 212
Systemstruktur
Anforderungen für den Zugriff 114
Auffüllen von Gruppen 122
Berechtigungssätze 114
Eigenes Unternehmen (Ebene) 112
Erstellung, automatisiert 115
festgelegt 113
Gruppen und manuelle Reaktivierungen 152
Gruppieren von Agenten 107
Kriterienbasierte Sortierung 118
Löschen von Systemen aus 113
Sammelgruppe 112
Struktur 111
Übergeordnete Gruppen und Vererbung 113
Untergeordnete Gruppen und Vererbung 113
Zuweisen von Richtlinien zu einer Gruppe 211
Systemstruktursortierung
Aktivieren 127, 128
Bei Agent-zu-Server-Kommunikation 119
IP-Adresse 120
Reihenfolge von Untergruppen 120
Server- und Systemeinstellungen 20, 119
Standardeinstellungen 121
System einmal sortieren 119
Tag-basierte Kriterien 120
Systemstruktursynchronisierung
Mit der Active Directory-Struktur 129
Planen 132

T

Tabellen, Arbeiten mit 22
Tabellenzeile, Aktivieren von Kontrollkästchen 24
Tag anwenden (Aktion) 141
Tag-basierte Sortierungskriterien 115, 120
Tag-Generator 141
Tag-Katalog 141
Tag-Kriterien ausführen (Aktion) 141
Tags 97
Ausschließen von Systemen von der automatischen Kennzeichnung 144
Bearbeiten, Löschen, Exportieren und Verschieben 142
Erstellen mit dem Tag-Generator 141
Erstellen, Löschen und Ändern von Untergruppen 143
Gruppensortierungskriterien 115
Kriterienbasiert 118
Kriterienbasierte Sortierung 127
Manuelle Anwendung von 146
Übernehmen 147, 148
Tags, Untergruppen
Erstellen, Löschen und Ändern 143
Technischer Support, Produktdokumentation finden 12
Test (Zweig)
Definition 68
Verwenden für neue DAT-Dateien und das Scan-Modul 240
Testmodus 38
Tool zur Datenmigration
Für Produktkompatibilitätsüberprüfung 183

U

UNC-Freigabe-Repositories
Aktivieren der Ordnerfreigabe 83
Bearbeiten 83
Erstellen und Konfigurieren 79
Informationen 67
Verwenden
Empfehlungen 84
Untergruppen
Kriterienbasiert 121
Richtlinienverwaltung 130

V

Vererbung
Anzeigen für Richtlinien 225
festgelegt 113
Richtlinieneinstellungen 205
Unterbrochene, zurücksetzen 226
Vererbung unterbrochen
Erstellen von Abfragen 220
Verteilte Repositories
Aktivieren der Ordnerfreigabe 83
Auswählen durch Agenten 90
Bearbeiten vorhandener 83
Begrenzte Bandbreite und 65
ePolicy Orchestrator-Komponenten 15
Erstellen und Konfigurieren 79
Hinzufügen zu ePolicy Orchestrator 80
Informationen 65, 67

Verteilte Repositories *(Fortsetzung)*
Löschen 83
Löschen von SuperAgent-Repositories 78
Nicht verwaltet 67
Nicht verwaltet, Kopieren von Inhalten 85
Ordner, erstellen 80
Replizieren von Paketen in SuperAgent-Repositories 78
SuperAgent (Tasks) 77
Typen 67
Verwaltete Systeme
Abfrage mit zusammengefassten Daten 279
Agenten-Server-Kommunikation 149
Ausbringungs-Tasks 235
Globale Aktualisierung 65
Installieren von Produkten 237
Richtlinienverwaltung 203
Richtlinienzuweisung 225
Sortierung, kriterienbasiert 118
Tasks 235
Verzeichnis, siehe Systemstruktur 129
Virusdefinitionsdateien 15
Vorherige (Zweig)
Definition 68
Speichern von Paketversionen 200
Verschieben von DAT- und Scan-Modul-Paketen 200
VPN-Verbindungen und geographische Gliederung 114

W

WAN-Verbindungen und geographische Gliederung 114
Wiederherstellung nach Systemausfall
Informationen benötigt für 252
Komponenten 314
Konfigurieren von Snapshots 250
Passphrase für die Schlüsselspeicherverschlüsselung 314
Wiederherstellung nach Systemausfall
Server-Einstellungen 324
Server-Task 250
Snapshot 313
Überblick 317
Was ist das? 313
Windows
Authentifizierung, konfigurieren 43, 46
Autorisierung, konfigurieren 47
Windows-Authentifizierung
Aktivieren 46
Strategien 45

Z

Zertifikatbasierte Authentifizierung
CRL-Datei aktualisieren 53
Erstellen eines selbstsignierten Zertifikats 57
Konvertieren von PVK- in PEM-Datei 60
Server-Zertifikatauthentifizierung ändern 51
Signiert von Drittanbieter-Zertifizierungsstelle 57
Verwenden von OpenSSL-Befehlen 59
Zuweisen von Problemen 309
Zuweisungsregeln
Agenten und Steuerungen 105
Zweig wechseln (Aktion) 240
Zweige
Aktuell 201
Manuelles Verschieben von Paketen 201
Test 240
Typen und Repositories 68
Verschieben oder Löschen von DAT- und Scan-Modul-Paketen 200
Vorherige 200
Zweig wechseln (Aktion) 240